Exhibit A

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MICHIGAN

JEFFREY SCHREIBER, individually and on behalf of all others similarly situated, Plaintiff, v. MAYO FOUNDATION FOR MEDICAL EDUCATION AND RESEARCH, Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Jeffrey Schreiber ("Plaintiff"), individually and on behalf of all others similarly situated, by and through his attorneys, makes the following allegations pursuant to the investigation of his counsel and based upon information and belief, except as to allegations specifically pertaining to himself and his counsel, which are based on personal knowledge.

INTRODUCTION

1.   Defendant Mayo Foundation for Medical Education and Research ("MFMER") rented, exchanged, and/or otherwise disclosed detailed information about Plaintiff's *Mayo Clinic Health Letter* healthletter subscription to data aggregators, data appenders, data cooperatives, and list brokers, among others, which in turn disclosed his information to aggressive advertisers, political

organizations, and non-profit companies. As a result, Plaintiff has received a barrage

of unwanted junk mail.   By renting, exchanging, and/or otherwise disclosing

Plaintiff's Private Reading Information (defined below) during the relevant pre-July

31, 2016 time period,[1] MFMER violated Michigan's Preservation of Personal

Privacy Act, H.B. 5331, 84th Leg. Reg. Sess., P.A. No. 378, §§ 1-4 (Mich. 1988),

id. § 5, added by H.B. 4694, 85th Leg. Reg. Sess., P.A. No. 206, § 1 (Mich. 1989)

(the "PPPA").[2]

---

[1]   The statutory period for this action is six years. *See* M.C.L. § 600.5813. The applicable six-year limitation period was tolled for 101 days pursuant to Executive Orders issued by the Governor of Michigan during the COVID-19 pandemic. *See* Mich. Executive Order No. 2020-58 ("[A]ll deadlines applicable to the commencement of all civil and probate actions and proceedings, including but not limited to any deadline for filing an initial pleading . . . are suspended as of March 10, 2020 and shall be tolled until the end of the declared states of disaster and emergency.") (emphasis added); Mich. Supreme Court Administrative Order No. 2020-3 ("For all deadlines applicable to the commencement of all civil and probate case types, including but not limited to the deadline for the initial filing of a pleading . . . any day that falls during the state of emergency declared by the Governor related to COVID-19 is not included.") (emphasis added); Mich. Executive Order No. 2020-122 (ending tolling period on June 20, 2020); Mich. Supreme Court Administrative Order No. 2020-18 (same); *see also Straus v. Governor*, 592 N.W.2d 53, 57 (Mich. 1999) (under Michigan law "the Governor's action [in issuing an Executive Order] has the status of enacted legislation"); *Blaha v. A.H. Robins & Co.*, 708 F.2d 238, 239 (6th Cir. 1983) ("Pursuant to the *Erie* doctrine, state statutes of limitations must be applied by federal courts sitting in diversity.").

[2]   In May 2016, the Michigan legislature amended the PPPA. *See* S.B. 490, 98th Leg., Reg. Sess., P.A. No. 92 (Mich. 2016) (codified at M.C.L. § 445.1711, *et seq.*). The May 2016 amendment to the PPPA, which became effective on July 31, 2016, does not apply retroactively to claims that accrued prior to its July 31, 2016 effective date. *See Boelter v. Hearst Commc'ns, Inc.*, 192 F. Supp. 3d 427, 439-41 (S.D.N.Y. 2016) (holding that "the amendment to the [PP]PA does not apply to Plaintiffs'

2

2. Documented evidence confirms these facts. For example, a list broker, NextMark, Inc. ("NextMark"), offers to provide renters access to the mailing list titled "MAYO CLINIC HEALTH LETTER Mailing List", which contains the Private Reading Information of all 449,162 of MFMER's active and recently expired U.S. subscribers at a base price of "$110.00/M [per thousand]," (i.e., 11 cents apiece), as shown in the screenshot below:

---

claims, and the Court will assess the sufficiency of those claims under the law as it was when Plaintiffs' claims accrued.") (citing *Landgraf v. USI Film Prods.*, 511 U.S. 224, 286 (1994)). Because the claims alleged herein accrued, and thus vested, prior to the July 31, 2016 effective date of the amended version of the PPPA, the pre-amendment version of the PPPA applies in this case. *See Horton v. GameStop, Corp.*, 380 F. Supp. 3d 679, 682-83 (W.D. Mich. 2018).

See **Exhibit A** hereto. The same or a substantially similar "data card" as the one shown above, with the same or similar rates and advertised demographic and personal information about each U.S. based purchaser of a subscription as listed above, was also publicly advertised by MFMER as far back as the beginning of 2015 and throughout the entire pre-July 31, 2016 time period – thus demonstrating that MFMER was renting, selling, exchanging, and otherwise disclosing all of its customers' Personal Reading Information (including Plaintiff's and all Class members' Personal Reading Information) to third parties during the relevant pre-July 31, 2016 time period.

3.   As a result of MFMER's practices of disclosing Plaintiff's Private Reading Information during the relevant pre-July 31, 2016 time period, Plaintiff saw a dramatic uptick of junk mail in his mailbox following his purchase of a subscription to *Mayo Clinic Health Letter* over the same time period.

4.   By renting, exchanging, or otherwise disclosing the Private Reading Information of all of its Michigan-based subscribers during the relevant pre-July 31, 2016 time period, MFMER violated the PPPA. Subsection 2 of the PPPA provides:

> [A] person, or an employee or agent of the person, engaged in the business of selling at retail, renting, or lending books or other written materials . . . shall not disclose to any person, other than the customer, a record or information concerning the purchase . . . of those materials by a customer that indicates the identity of the customer.

PPPA § 2.

5.   Accordingly, Plaintiff brings this Class Action Complaint against

MFMER for its intentional and unlawful disclosure of its customers' Private

Reading Information in violation of the PPPA.

NATURE OF THE CASE

6.   To supplement its revenues, MFMER rents, exchanges, or otherwise

discloses all of its customers' information—including their full names, titles of

publications subscribed to, and home addresses (collectively "Private Reading

Information"), as well as myriad other categories of individualized data and

demographic information such as gender—to data aggregators, data appenders, data

cooperatives, and other third parties without the written consent of its customers.

MFMER continuously engaged in these same practices (disclosing its entire

database of its customers' Personal Reading Information to third parties, at least as

frequently as once a month) since at least as far back as 2015 through the present,

including for the entire pre-July 31, 2016 time period.

7.   By renting, exchanging, or otherwise disclosing – rather than selling –

its customers' Private Reading Information, MFMER is able to disclose the

information time and time again to countless third parties.

8.   MFMER's disclosure of Private Reading Information and other

individualized information is not only unlawful, but also dangerous because it allows

for the targeting of particularly vulnerable members of society.

9.   While MFMER profits handsomely from the unauthorized rental, exchange, and/or disclosure of its customers' Private Reading Information and other individualized information, it does so at the expense of its customers' statutory privacy rights (afforded by the PPPA) because MFMER does not obtain its customers' written consent prior to disclosing their Private Reading Information.

PARTIES

10.   Plaintiff Jeffrey Schreiber is a natural person and citizen of the State of Michigan and resides in Chassell, Michigan. Plaintiff was a subscriber to *Mayo Clinic Health Letter* healthletter, including prior to July 31, 2016. *Mayo Clinic Health Letter* healthletter is published by MFMER. While residing in, a citizen of, and present in Michigan, Plaintiff purchased his subscription to *Mayo Clinic Health Letter* healthletter directly from MFMER. Prior to and at the time Plaintiff subscribed to *Mayo Clinic Health Letter*, MFMER did not notify Plaintiff that it discloses the Private Reading Information of its customers, and Plaintiff has never authorized MFMER to do so. Furthermore, Plaintiff was never provided any written notice that MFMER rents, exchanges, or otherwise discloses its customers' Private Reading Information, or any means of opting out. Since subscribing to *Mayo Clinic Health Letter*, and during the relevant pre-July 31, 2016 time period, MFMER disclosed, without the requisite consent or prior notice, Plaintiff's Private Reading

6

Information to data aggregators, data appenders, and/or data cooperatives, who then supplemented that information with data from their own files. Moreover, during that same period, MFMER rented or exchanged mailing lists containing Plaintiff's Private Reading Information to third parties seeking to contact MFMER subscribers, without first obtaining the requisite written consent from Plaintiff or even giving him prior notice of the rentals, exchanges, and/or other disclosures.

11.   Defendant Mayo Foundation for Medical Education and Research is a Minnesota corporation with its headquarters and principal place of business in Rochester, Minnesota. MFMER does business throughout Michigan and the entire United States. MFMER is the publisher of various medical books and other publications, including but not limited to *Mayo Clinic Health Letter*.

JURISDICTION AND VENUE

12.   This Court has subject matter jurisdiction over this civil action pursuant to 28 U.S.C. § 1332(d) because there are more than 100 class members and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest, fees, and costs, and at least one Class member is a citizen of a state different from Defendant.

13.   The Court has personal jurisdiction over MFMER because Plaintiff's claims arose in substantial part from actions and omissions in Michigan, including from Plaintiff's purchase of a *Mayo Clinic Health Letter* subscription in Michigan,

MFMER's direction of such *Mayo Clinic Health Letter* subscription into Michigan, and MFMER's failure to obtain Plaintiff's written consent in Michigan prior to disclosing his Private Reading Information, including his residential address in Michigan, to another person, the effects of which were felt from within Michigan by a citizen and resident of Michigan. Personal jurisdiction also exists over MFMER in Michigan because MFMER conducts substantial business within Michigan, such that MFMER has significant, continuous, and pervasive contacts with the State of Michigan.

14.   Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Plaintiff resides in this judicial District, MFMER does substantial business in this judicial District, MFMER is subject to personal jurisdiction in this judicial District, and a substantial part of the events giving rise to Plaintiff's claims took place within this judicial District.

FACTUAL BACKGROUND

Michigan's Preservation of Personal Privacy Act

15.   In 1988, members of the United States Senate warned that records of consumers' purchases and rentals of audiovisual and publication materials offer "a window into our loves, likes, and dislikes," and that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance."

S. Rep. No. 100-599 at 7–8 (1988) (statements of Sens. Simon and Leahy, respectively).

16.   Recognizing the need to further protect its citizens' privacy rights, Michigan's legislature enacted the PPPA to protect "privacy with respect to the purchase, rental, or borrowing of certain materials," by prohibiting companies from disclosing certain types of sensitive consumer information. H.B. No. 5331, 1988 Mich. Legis. Serv. 378 (West).

17.   Subsection 2 of the PPPA states:

> [A] person, or an employee or agent of the person, engaged in the business of selling at retail, renting, or lending books or other written materials . . . *shall not disclose* to any person, other than the customer, a record or information concerning the purchase . . . of those materials by a customer that indicates the identity of the customer.

PPPA § 2 (emphasis added).

18.   Michigan's protection of reading information reflects the "gut feeling that people ought to be able to read books and watch films without the whole world knowing," and recognizes that "[b]ooks and films are the intellectual vitamins that fuel the growth of individual thought. The whole process of intellectual growth is one of privacy—of quiet, and reflection. This intimate process should be protected from the disruptive intrusion of a roving eye." S. Rep. No. 100–599, at 6 (Statement of Rep. McCandless).

19.   As Senator Patrick Leahy recognized in proposing the Video and Library Privacy Protection Act (later codified as the Video Privacy Protection Act, 18 U.S.C. § 2710), "[i]n practical terms our right to privacy protects the choice of movies that we watch with our family in our own homes. And it protects the selection of books that we choose to read." 134 Cong. Rec. S5399 (May 10, 1988).

20.   Senator Leahy also explained why choices in movies and reading materials are so private: "These activities . . . reveal our likes and dislikes, our interests and our whims. They say a great deal about our dreams and ambitions, our fears and our hopes. They reflect our individuality, and they describe us as people." *Id.*

21.   Michigan's passage of the PPPA also established as a matter of law "that a person's choice in reading, music, and video entertainment is a private matter, and not a fit subject for consideration by gossipy publications, employers, clubs, or anyone else for that matter." *Privacy: Sales, Rentals of Videos, etc.*, House Legislative Analysis Section, H.B. No. 5331, Jan. 20, 1989 (attached hereto as **Exhibit B**).

22.   Despite the fact that thousands of Michigan residents subscribe to MFMER's publications, MFMER disregarded its legal responsibility by systematically violating the PPPA.

The Private Information Market:
Consumers' Private Information Has Real Value

23.   In 2001, Federal Trade Commission ("FTC") Commissioner Orson

Swindle remarked that "the digital revolution . . . has given an enormous capacity

to the acts of collecting and transmitting and flowing of information, unlike anything

we've ever seen in our lifetimes . . . [and] individuals are concerned about being

defined by the existing data on themselves."[3]

24.   More than a decade later, Commissioner Swindle's comments ring

truer than ever, as consumer data feeds an information marketplace that supports a

$26 billion dollar per year online advertising industry in the United States.[4]

25.   The FTC has also recognized that consumer data possesses inherent

monetary value within the new information marketplace and publicly stated that:

> Most consumers cannot begin to comprehend the types
> and amount of information collected by businesses, or why
> their information may be commercially valuable. Data is
> currency. The larger the data set, the greater potential for

---

[3]   **Exhibit C**, The Information Marketplace: Merging and Exchanging
Consumer   Data   (Mar.   13,   2001),   at   8:15-11:16,   *available   at*
https://www.ftc.gov/sites/default/files/documents/public_events/information-
marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last visited
July 30, 2021).

[4]   *See* **Exhibit D**, Web's Hot New Commodity: Privacy, WSJ (Feb. 28, 2011),
http://online.wsj.com/article/SB10001424052748703529004576160764037920274
.html (last visited July 30, 2021).

analysis—and profit.[5]

26.   In fact, an entire industry exists while companies known as data aggregators purchase, trade, and collect massive databases of information about consumers. Data aggregators then profit by selling this "extraordinarily intrusive" information in an open and largely unregulated market.[6]

27.   The scope of data aggregators' knowledge about consumers is immense: "If you are an American adult, the odds are that [they] know[] things like your age, race, sex, weight, height, marital status, education level, politics, buying habits, household health worries, vacation dreams—and on and on."[7]

28.   Further, "[a]s use of the Internet has grown, the data broker industry has already evolved to take advantage of the increasingly specific pieces of

---

[5]   **Exhibit E**, Statement of FTC Commissioner Pamela Jones Harbour (Dec. 7, 2009), at 2, *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited July 30, 2021).

[6]   *See* **Exhibit F**, Martha C. White, *Big Data Knows What You're Doing Right Now*, TIME.com (July 31, 2012), http://moneyland.time.com/2012/07/31/big-data-knows-what-youre-doing-right-now/ (last visited July 30, 2021).

[7]   **Exhibit G**, Natasha Singer, *You for Sale: Mapping, and Sharing, the Consumer Genome*, N.Y. Times (June 16, 2012), *available at* https://www.immagic.com/eLibrary/ARCHIVES/GENERAL/GENPRESS/N120616S.pdf (last visited July 30, 2021).

information about consumers that are now available."[8]

29.   Recognizing the serious threat the data mining industry poses to consumers' privacy, on July 25, 2012, the co-Chairmen of the Congressional Bi-Partisan Privacy Caucus sent a letter to nine major data brokerage companies seeking information on how those companies collect, store, and sell their massive collections of consumer data.[9]

30.   In their letter, the co-Chairmen recognized that "[b]y combining data from numerous offline and online sources, data brokers have developed hidden dossiers on every U.S. consumer," which "raises a number of serious privacy concerns."[10]

31.   Data aggregation is especially troublesome when consumer information is sold to direct-mail advertisers. In addition to causing waste and inconvenience, direct-mail advertisers often use consumer information to lure

---

[8]   **Exhibit H**, Letter from Senator John D. Rockefeller IV, Chairman, Senate Committee on Commerce, Science, and Transportation, to Scott E. Howe, Chief Executive Officer, Acxiom (Oct. 9, 2012) *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=3bb94703-5ac8-4157-a97b-a658c3c3061c (last visited July 30, 2021).

[9]   *See* **Exhibit I**, *Bipartisan Group of Lawmakers Query Data Brokers About Practices Involving Consumers' Personal Information*, Website of Senator Ed Markey (July 24, 2012), http://www.markey.senate.gov/news/press-releases/bipartisan-group-of-lawmakers-query-data-brokers-about-practices-involving-consumers-personal-information (last visited July 30, 2021).

[10]   *Id.*

unsuspecting consumers into various scams,[11] including fraudulent sweepstakes,

charities, and buying clubs. Thus, when companies like MFMER share information

with data aggregators, data cooperatives, and direct-mail advertisers, they contribute

to the "[v]ast databases" of consumer data that are often "sold to thieves by large

publicly traded companies," which "put[s] almost anyone within the reach of

fraudulent telemarketers" and other criminals.[12]

32.   Information disclosures like those made by MFMER are particularly

dangerous to the elderly. "Older Americans are perfect telemarketing customers,

analysts say, because they are often at home, rely on delivery services, and are lonely

for the companionship that telephone callers provide."[13] The FTC notes that "[t]he

elderly often are the deliberate targets of fraudulent telemarketers who take

advantage of the fact that many older people have cash reserves or other assets to

spend on seemingly attractive offers."[14] Indeed, an entire black market exists where

---

[11]   *See* **Exhibit J**, *Prize Scams*, Federal Trade Commission, http://www.consumer.ftc.gov/articles/0199-prize-scams (last visited July 30, 2021).

[12]   **Exhibit K**, Charles Duhigg, *Bilking the Elderly, With a Corporate Assist*, N.Y. Times, May 20, 2007, *available at* http://www.nytimes.com/2007/05/20/business/20tele.html (last visited July 30, 2021).

[13]   *Id.*

[14]   **Exhibit L**, *Fraud Against Seniors: Hearing before the Senate Special Committee on Aging* (August 10, 2000) (prepared statement of the FTC), *available at*   https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-

the private information of vulnerable elderly Americans is exchanged.

33.   Thus, information disclosures like MFMER's are particularly troublesome because of their cascading nature: "Once marked as receptive to [a specific] type of spam, a consumer is often bombarded with similar fraudulent offers from a host of scam artists."[15]

34.   MFMER is not alone in jeopardizing its subscribers' privacy and well-being in exchange for increased revenue: disclosing subscriber information to data aggregators, data appenders, data cooperatives, direct marketers, and other third parties is a widespread practice in the publishing industry.

35.   Thus, as consumer data has become an ever-more valuable commodity, the data mining industry has experienced rapid and massive growth. Unfortunately for consumers, this growth has come at the expense of their most basic privacy rights.

Consumers Place Monetary Value on Their Privacy and Consider Privacy Practices When Making Purchases

36.   As the data aggregation and cooperative industry has grown, so too have consumer concerns regarding the privacy of their information.

37.   A recent survey conducted by Harris Interactive on behalf of

---

statement-federal-trade-commission-fraud-against-seniors/agingtestimony.pdf (last visited July 30, 2021).

[15]   *See id.*

TRUSTe, Inc. showed that 89 percent of consumers polled avoid doing business with companies who they believe do not protect their privacy online.[16] As a result, 81 percent of smartphone users polled said that they avoid using smartphone apps that they don't believe protect their privacy online.[17]

38.   Thus, as consumer privacy concerns grow, consumers are increasingly incorporating privacy concerns and values into their purchasing decisions and companies viewed as having weaker privacy protections are forced to offer greater value elsewhere (through better quality and/or lower prices) than their privacy-protective competitors.

39.   In fact, consumers' private information has become such a valuable commodity that companies are beginning to offer individuals the opportunity to sell their information themselves.[18]

40.   These companies' business models capitalize on a fundamental tenet underlying the consumer information marketplace: consumers recognize the

---

[16]   *See* **Exhibit M**, *2014 TRUSTe US Consumer Confidence Privacy Report*, TRUSTe, http://www.theagitator.net/wp-content/uploads/012714_ConsumerConfidenceReport_US1.pdf (last visited July 30, 2021).

[17]   *Id.*

[18]   *See* **Exhibit N**, Joshua Brustein, *Start-Ups Seek to Help Users Put a Price on Their Personal Data*, N.Y. Times (Feb. 12, 2012), *available at* http://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html (last visited July 30, 2021).

economic value of their private data. Research shows that consumers are willing to

pay a premium to purchase services from companies that adhere to more stringent

policies of protecting their data.[19]

41.   Thus, in today's economy, individuals and businesses alike place a

real, quantifiable value on consumer data and corresponding privacy rights.[20]

MFMER Unlawfully Rents, Exchanges, and Discloses Its Customers' Private Reading Information

42.   MFMER maintains a vast digital database comprised of its customers'

Private Reading Information. MFMER discloses its customers' Private Reading

Information to data aggregators and appenders, who then supplement that

information with additional sensitive private information about each MFMER

customer, including his or her gender. (*See, e.g.*, **Exhibit A**).

43.   MFMER then rents and/or exchanges its mailing lists—which include

subscribers' Private Reading Information identifying which individuals purchased

---

[19]   *See* **Exhibit O**, Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (2011); discussed in European Network and Information Security Agency, *Study on monetising privacy* (Feb. 27, 2012), *available at* https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy (last visited July 30, 2021).

[20]   *See* **Exhibit P**, Hann, *et al.*, *The Value of Online Information Privacy: An Empirical Investigation* (Oct. 2003) at 2, *available at* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.321.6125&rep=rep1&type=pdf (last visited July 30, 2021) ("The real policy issue is not whether consumers value online privacy. It is obvious that people value online privacy.").

subscriptions to particular healthletters, and can include the sensitive information obtained from data aggregators and appenders—to other data aggregators and appenders, other consumer-facing businesses, non-profit organizations seeking to raise awareness and solicit donations, and to political organizations soliciting donations, votes, and volunteer efforts. (*See* **Exhibit A**).

44.   MFMER also discloses its customers' Private Reading Information to data cooperatives, who in turn give MFMER access to their own mailing list databases.

45.   As a result of MFMER's data compiling and sharing practices, companies can purchase and/or obtain mailing lists from MFMER that identify MFMER's customers by their most intimate details such as their gender. MFMER's disclosures of such sensitive and private information puts consumers, especially the more vulnerable members of society, at risk of serious harm from scammers.

46.   MFMER does not seek its customers' prior consent, written or otherwise, to any of these disclosures and its customers remain unaware that their Private Reading Information and other sensitive information is being rented and exchanged on the open market.

47.   During the relevant pre-July 31, 2016 time period, consumers purchased subscriptions to MFMER's publications through numerous media outlets, including the Internet, telephone, or traditional mail. Regardless of how the

consumer subscribed, MFMER never required the individual to read or affirmatively agree to any terms of service, privacy policy, or information-sharing policy during the relevant pre-July 31, 2016 time period. Consequently, during the relevant pre-July 31, 2016 time period, MFMER uniformly failed to obtain any form of consent from – or even provide effective notice to – its customers before disclosing their Private Reading Information.

48.   As a result, MFMER disclosed its customers' Private Reading Information – including their reading habits and preferences that can "reveal intimate facts about our lives, from our political and religious beliefs to our health concerns"[21] – to anybody willing to pay for it.

49.   By and through these actions, MFMER has intentionally disclosed to third parties its Michigan customers' Private Reading Information without consent, in direct violation of the PPPA.

<div align="center">

CLASS ACTION ALLEGATIONS

</div>

50.   Plaintiff seeks to represent a class defined as all Michigan residents who, at any point during the relevant pre-July 31, 2016 time period, had their Private Reading Information disclosed to third parties by MFMER without consent (the "Class"). Excluded from the Class is any entity in which Defendant has a controlling

---

[21]   **Exhibit Q**, *California's Reader Privacy Act Signed into Law*, Electronic Frontier Foundation (Oct. 3, 2011), https://www.eff.org/press/archives/2011/10/03 (last visited July 30, 2021).

interest, and officers or directors of Defendant.

51.   Members of the Class are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class number in the thousands. The precise number of Class members and their identities are unknown to Plaintiff at this time but may be determined through discovery. Class members may be notified of the pendency of this action by mail and/or publication through the distribution records of Defendant.

52.   Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Common legal and factual questions include, but are not limited to: (a) whether MFMER is a "retailer or distributor" of publications (*i.e.*, healthletters); (b) whether MFMER obtained consent before disclosing to third parties Plaintiff's and the Class's Private Reading Information; and (c) whether MFMER's disclosure of Plaintiff's and the Class's Private Reading Information violated the PPPA.

53.   The claims of the named Plaintiff are typical of the claims of the Class in that the named Plaintiff and the Class suffered invasions of their statutorily protected right to privacy (as afforded by the PPPA) as a result of Defendant's uniform wrongful conduct, based upon Defendant's disclosure of Plaintiff's and the Class's Private Reading Information.

54.   Plaintiff is an adequate representative of the Class because his interests

do not conflict with the interests of the Class members he seeks to represent, he has

retained competent counsel experienced in prosecuting class actions, and he intends

to prosecute this action vigorously. The interests of Class members will be fairly

and adequately protected by Plaintiff and his counsel.

55.   The class mechanism is superior to other available means for the fair

and efficient adjudication of the claims of Class members. Each individual Class

member may lack the resources to undergo the burden and expense of individual

prosecution of the complex and extensive litigation necessary to establish

Defendant's liability. Individualized litigation increases the delay and expense to

all parties and multiplies the burden on the judicial system presented by the complex

legal and factual issues of this case. Individualized litigation also presents a potential

for inconsistent or contradictory judgments. In contrast, the class action device

presents far fewer management difficulties and provides the benefits of single

adjudication, economy of scale, and comprehensive supervision by a single court on

the issue of Defendant's liability. Class treatment of the liability issues will ensure

that all claims and claimants are before this Court for consistent adjudication of the

liability issues.

CAUSE OF ACTION
Violation of Michigan's Preservation of Personal Privacy Act
(PPPA § 2)

56.   Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

57.   Plaintiff brings this claim individually and on behalf of members of the Class against Defendant MFMER.

58.   As a healthletter publisher that sells subscriptions to consumers, MFMER is engaged in the business of selling written materials at retail. *See* PPPA § 2.

59.   By purchasing a subscription to *Mayo Clinic Health Letter* healthletter, Plaintiff purchased written materials directly from MFMER. *See* PPPA § 2.

60.   Because Plaintiff purchased written materials directly from MFMER, he is a "customer" within the meaning of the PPPA. *See* PPPA § 1.

61.   At various times during the pre-July 31, 2016 time period, MFMER disclosed Plaintiff's Private Reading Information, which identified him as a *Mayo Clinic Health Letter* customer, in at least three ways.

62.   First, MFMER disclosed mailing lists containing Plaintiff's Private Reading Information to data aggregators and data appenders, who then supplemented the mailing lists with additional sensitive information from their own databases, before sending the mailing lists back to MFMER.

63.   Second, MFMER disclosed mailing lists containing Plaintiff's Private

Reading Information to data cooperatives, who in turn gave MFMER access to their

own mailing list databases.

64.   Third, MFMER rented and/or exchanged its mailing lists containing

Plaintiff's Private Reading Information—enhanced with additional information

from data aggregators and appenders—to third parties, including other consumer-

facing companies, direct-mail advertisers, and organizations soliciting monetary

contributions, volunteer work, and votes.

65.   Because the mailing lists included the additional information from the

data aggregators and appenders, the lists were more valuable, and MFMER was able

to increase its profits gained from the mailing list rentals and/or exchanges.

66.   By renting, exchanging, or otherwise disclosing its customer lists,

during the relevant pre-July 31, 2016 time period, MFMER disclosed to persons

other than Plaintiff records or information concerning his purchase of written

materials from MFMER. *See* PPPA § 2.

67.   The information MFMER disclosed indicates Plaintiff's name and

address, as well as the fact that he subscribed to *Mayo Clinic Health Letter*.

Accordingly, the records or information disclosed by MFMER indicated Plaintiff's

identity. *See* PPPA § 2.

68.   Plaintiff and the members of the Class never consented to MFMER

disclosing their Private Reading Information to anyone.

69.   Worse yet, Plaintiff and the members of the Class did not receive notice before MFMER disclosed their Private Reading Information to third parties.

70.   MFMER's disclosures of Plaintiff's and the Class's Private Reading Information during the relevant pre-July 31, 2016 time period were not made pursuant to a court order, search warrant, or grand jury subpoena.

71.   MFMER's disclosures of Plaintiff's and the Class's Private Reading Information during the relevant pre-July 31, 2016 time period were not made to collect payment for their subscriptions.

72.   MFMER's disclosures of Plaintiff's Private Reading Information during the relevant pre-July 31, 2016 time period were made to data aggregators, data appenders, data cooperatives, direct-mail advertisers, and organizations soliciting monetary contributions, volunteer work, and votes—all in order to increase MFMER's revenue. Accordingly, MFMER's disclosures were not made for the exclusive purpose of marketing goods and services directly to Plaintiff and the members of the Class.

73.   By disclosing Plaintiff's and the Class's Private Reading Information during the relevant pre-July 31, 2016 time period, MFMER violated Plaintiff's and the Class's statutorily protected right to privacy in their reading habits. *See* PPPA § 2.

74.   As a result of MFMER's unlawful disclosure of their Private Reading

Information, Plaintiff and the members of the Class have suffered invasions of their

statutorily protected right to privacy (afforded by the PPPA). On behalf of himself

and the Class, Plaintiff seeks: (1) $5,000.00 to Plaintiff and each Class member

pursuant to PPPA § 5(a); and (2) costs and reasonable attorneys' fees pursuant to

PPPA § 5(b).

<div align="center">

PRAYER FOR RELIEF

</div>

WHEREFORE, Plaintiff, individually and on behalf of all others similarly

situated, seeks a judgment against Defendant as follows:

A.   For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

B.   For an order declaring that Defendant's conduct as described herein violated the Preservation of Personal Privacy Act;

C.   For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

D.   For an award of $5,000 to Plaintiff and each Class member, as provided by the Preservation of Personal Privacy Act, PPPA § 5(a);

E.   For prejudgment interest on all amounts awarded; and

F.   For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit.

<div align="center">

25

</div>

JURY DEMAND

Plaintiff demands a trial by jury on all causes of action and issues so triable.

Dated: September 26, 2022   Respectfully submitted,

JEFFREY SCHREIBER,

/s/ *E. Powell Miller*
E. Powell Miller (P39487)
Sharon S. Almonrode (P33938)
THE MILLER LAW FIRM, P.C.
950 W. University Drive, Suite 300
Rochester, MI 48307
Tel: 248-841-2200
epm@millerlawpc.com
ssa@millerlawpc.com

Joseph I. Marchese
Philip L. Fraietta
BURSOR & FISHER, P.A.
888 Seventh Avenue
New York, New York 10019
Tel: 646.837.7150
Fax: 212.989.9163
jmarchese@bursor.com
pfraietta@bursor.com

Frank S. Hedin
Arun G. Ravindran
HEDIN HALL LLP
1395 Brickell Avenue, Suite 1140
Miami, Florida 33131
Tel: 305.357.2107
Fax: 305.200.8801
fhedin@hedinhall.com
aravindran@hedinhall.com

Counsel for Plaintiff and the Putative Class

26

INDEX OF EXHIBITS

A.   MAYO CLINIC HEALTH LETTER Mailing List

B.   *Privacy: Sales, Rentals of Videos, etc.*, House Legislative Analysis Section, H.B. No. 5331, Jan. 20, 1989

C.   The Information Marketplace: Merging and Exchanging Consumer Data (Mar. 13, 2001)

D.   Web's Hot New Commodity: Privacy, WSJ (Feb. 28, 2011)

E.   Statement of FTC Commissioner Pamela Jones Harbour (Dec. 7, 2009)

F.   Martha C. White, *Big Data Knows What You're Doing Right Now*, TIME.com (July 31, 2012)

G.   Natasha Singer, *You for Sale: Mapping, and Sharing, the Consumer Genome*, N.Y. Times (June 16, 2012)

H.   Letter from Senator John D. Rockefeller IV, Chairman, Senate Committee on Commerce, Science, and Transportation, to Scott E. Howe, Chief Executive Officer, Acxiom (Oct. 9, 2012)

I.   *Bipartisan Group of Lawmakers Query Data Brokers About Practices Involving Consumers' Personal Information*, Website of Senator Ed Markey (July 24, 2012)

J.   *Prize Scams*, Federal Trade Commission

K.   Charles Duhigg, *Bilking the Elderly, With a Corporate Assist*, N.Y. Times, May 20, 2007

L.   *Fraud Against Seniors: Hearing before the Senate Special Committee on Aging* (August 10, 2000)

M.   *2014 TRUSTe US Consumer Confidence Privacy Report*, TRUSTe

N.   Joshua Brustein, *Start-Ups Seek to Help Users Put a Price on Their Personal Data*, N.Y. Times (Feb. 12, 2012)

O.   European Network and Information Security Agency, *Study on monetizing privacy* (Feb. 27, 2012)

P.   Hann, *et al.*, *The Value of Online Information Privacy: An Empirical Investigation* (Oct. 2003)

Q.   *California's Reader Privacy Act Signed into Law*, Electronic Frontier Foundation (Oct. 3, 2011)

Exhibit A

MAYO CLINIC HEALTH LETTER Mailing List

Mayo Foundation for Medical Education and Research. Mayo Clinic newsletters are backed by a century of patient care medical research and experience at one of the world's foremost medical centers. This eight page monthly newsletter provided reliable, accurate and practical information on today's health and medical news: Fitness & exercise, medical treatment breakthroughs, nutrition & healthy eating, tips on treating and preventing hundreds of illnesses. http://www.mayoclinic.com

Get Count   **Get Pricing**   **Get More Information**

SEGMENTS	COUNTS THROUGH 07/29/2022	POPULARITY:	===== 100
449,162 TOTAL UNIVERSE / BASE RATE	$110.00/M	MARKET:	CONSUMER
23,115 MONTHLY HOTLINE	+ $15.00/M	CHANNELS:	[≥]
66,894 QUARTERLY HOTLINE	+ $10.00/M	SOURCE:	DIRECT MAIL
146,563 6 MONTH HOTLINE	+ $8.00/M	PRIVACY:	UNKNOWN
449,162 ACTIVE US SUBS	$110.00/M	DMA?:	YES - MEMBER
35,164 12 MONTH COA	+ $10.00/M	STATUS:	PREFERRED PROVIDER
290,435 12 MONTH EXPIRES	$80.00/M	GEO:	USA

DESCRIPTION

GENDER: 46% FEMALE 38% MALE

Mayo Clinic
NEWSLETTER AND BOOK BUYERS

Mayo Foundation for Medical Education and Research.

Mayo Clinic newsletters are backed by a century of patient care medical research and experience at one of the world's foremost medical centers.

This eight page monthly newsletter provided reliable, accurate and practical information on today's health and medical news: Fitness & exercise, medical treatment breakthroughs, nutrition & healthy eating, tips on treating and preventing hundreds of illnesses.

www.mayoclinic.com

SELECTS	
1 MONTH HOTLINE	$15.00/M
3 MONTH HOTLINE	$10.00/M
6 MONTH HOTLINE	$8.00/M
CHANGE OF ADDRESS	$10.00/M
GENDER/SEX	$10.00/M
SCF	$10.00/M
STATE	$10.00/M
ZIP	$10.00/M

ADDRESSING	
KEY CODING	$10.00/M
CARTRIDGE (FLAT FEE)	$30.00/F
DISKETTE (FLAT FEE)	$75.00/F
EMAIL DELIVERY (FLAT FEE)	$75.00/F
FUNDRAISING/NON-PROFIT KEYING	$10.00/M
MODEM/FTP/BBS (FLAT FEE)	$75.00/F
RUN CHARGES	$12.00/M
ZIP TAPE (FLAT FEE)	$100.00/F
ZIP+4	$3.00/M

Orders which need zip file breakouts of 10 or more will incur a $100/F fee.

Subscriber Profiles:
Mature - age 60+
College educated
Above average incomes

Catalog and fundraiser rates are available.

All orders cancelled after merge and/or mail date will be billed at full rental rate. Orders cancelled prior to merge will be billed a $150/F fee plus $12/M run charges and all applicable selection charges. List owner/manager needs to be notified of any cut backs or cancellations before the merge happens.

RELATED LISTS
WILAND
☐ NONPROFIT/FUNDRAISING/DONOR DATABASE
☐ SPECIAL OLYMPICS INTERNATIONAL
☐ AMERICAN LUNG ASSOCIATION DONOR MASTERFILE
☐ ALZHEIMER'S DISEASE RESEARCH
☐ I-BEHAVIOR DATABASE
☐ CONSUMER REPORTS
☐ NATIONAL FOUNDATION FOR CANCER RESEARCH
☐ CONSUMER REPORTS ON HEALTH
☐ AICR - AMERICAN INSTITUTE FOR CANCER RESEARCH DONORS
☐ LEUKEMIA & LYMPHOMA SOCIETY, THE

Exhibit B

**House
Legislative
Analysis
Section**

Washington Square Building, Suite 1025
Lansing, Michigan 48909
Phone: 517/373-6466

PRIVACY: SALES, RENTALS OF VIDEOS, ETC.

House Bill 5331 as enrolled
Second Analysis (1-20-89)

Sponsor: Rep. David Honigman
House Committee: Judiciary
Senate Committee: Judiciary

THE APPARENT PROBLEM:

During the period when Congressional confirmation hearings were being held on the nomination of Robert Bork to the Supreme Court, a Washington weekly obtained and published a list of videotapes rented under Bork's wife's account. Many found this to be an unwarranted invasion of privacy, and the incident prompted the introduction in Congress of a bill to protect the privacy of those who rent or buy videotapes. Many in Michigan also believe that one's choice in videos, records, and books is nobody's business but one's own, and suggest the enactment of a statute to explicitly protect a consumer's privacy in buying and borrowing such items.

THE CONTENT OF THE BILL:

The bill would create a new public act to preserve personal privacy with respect to the purchase, rental, or borrowing of written materials, sound recordings, and video recordings. Except as otherwise provided by law, a retailer, lender, or renter of such items could not disclose information — such as selections made — on a particular customer to any person other than that customer. Such information could be disclosed with the customer's written permission, under a court order, to the extent reasonably necessary to collect past-due payment, for the exclusive purpose of marketing goods and services directly to the consumer, or under a search warrant. Violation of the bill would be a misdemeanor.

FISCAL IMPLICATIONS:

The House Fiscal Agency says that the bill would have no fiscal implications. (1-18-89)

ARGUMENTS:

For:

The bill would recognize that a person's choice in reading, music, and video entertainment is a private matter, and not a fit subject for consideration by gossipy publications, employers, clubs, or anyone else, for that matter. The bill would complement the Library Privacy Act, which exempts library records on a person from disclosure under the Freedom of Information Act and prohibits disclosure absent a court order or the individual's consent.

Response: The bill, while laudable in its aims, may be unnecessary for libraries, which already are subject to civil penalties for violating the Library Privacy Act.

Against:

The bill could offer more in the way of recourse for injured parties if it provided for civil damages as well as criminal misdemeanor penalties. Civil remedies not only offer a person recompense for harm done: they free a person from having to rely on a prosecutor's office to pursue a case.

H.B. 5331 (1-20-89)

Exhibit C

1

 1   FEDERAL TRADE COMMISSION

 2

 3

 4

 5

 6   Public Workshop:

 7

 8

 9

10   THE INFORMATION MARKETPLACE:

11   MERGING AND EXCHANGING CONSUMER DATA

12

13

14

15   March 13, 2001

16

17

18

19   Federal Trade Commission

20   6th and Pennsylvania Avenue, N.W.

21   Washington, D.C.

22

23

24

25

                      For The Record, Inc.
                       Waldorf, Maryland
                        (301) 870-8025

```
 1                      I N D E X

 2

 3   SESSION:                                   PAGE:

 4   Opening Remarks
```

```
21

22

23

24

25
```

3

1   P R O C E E D I N G S

2   - - - - - -

3   MR. WINSTON: Let me introduce myself, I'm

4   Joel Winston, Acting Associate Director for

5   Financial Practices at the FTC, and I want to

6   welcome all of you to the Federal Trade Commission,

7   and give a special greeting to those people who are

8   listening in on our audiocast on the website,

9   ftc.gov.

10   Now, there are several members of the

11   Commission who are going to be giving some opening

12   remarks this morning, and I would like to introduce

13   first Chairman Robert Pitofsky. Chairman Pitofsky

14   has served as chairman of the FTC since April of

15   1995, and he will be beginning the proceedings.

16   Mr. Chairman?

17   CHAIRMAN PITOFSKY: Good morning, everyone,

18   and welcome to another of the Federal Trade

19   Commission's workshops. This one, we have entitled

20   The Information Marketplace: Merger and Exchange

21   of Consumer Data.

22   I don't think I have to belabor the point

23   with this audience that privacy, especially privacy

24   in the commercial marketplace, is and remains a

25   very important issue.

1   If you take polls, you find today, just as

2   you did three and four years ago, that somewhere

3   between 88 and 92 percent of consumers when asked

4   what their concerns were about doing business,

5   buying online, will say that they have

6   reservations, and think it's not a secure

7   marketplace. They're not giving their credit card

8   online without having some knowledge of how it's

9   going to be used.

10   As a result, you now have, I think, just

11   since Congress reconvened, something like a dozen

12   bills addressing various issues relating to privacy

13   in the commercial context.

14   But let me position this workshop. We are

15   not looking for enforcement targets for companies

16   that may be invading unfairly or deceptively

17   consumer rights, and we're not looking for

18   legislative proposals.

19   This is another kind of workshop, and it's

20   like many that we've conducted in the past five or

21   six years. We're trying to find out in a new area,

22   a fast-changing dynamic area, what's going on, so

23   that we are informed about the kind of issues that

24   eventually we'll be called upon to address.

25   We did that with our earliest privacy

5

1   workshops, just to find out how personally

2   identifiable information was collected and whether

3   or not it was being sold. We did it with

4   profiling, more recently B2B commerce on the

5   Internet, and wireless technologies.

6   In this instance, we would like to be able

7   to take the measure of the extent and the ways in

8   which firms exchange information and data that

9   create consumer profiles; not necessarily only the

10   information the firm collects itself, but

11   information that someone else collects that then

12   becomes merged into a firm's database.

13   How is that information used commercially?

14   Is it used commercially? And if so, in what

15   fashion? What is the source of the data? Is it

16   mostly online, is it offline, is it a combination

17   of the two? Does it come from public records,

18   private records, a combination of the two?

19   We know that the ability of firms to

20   collect data has been enhanced dramatically over

21   the last five to ten years, and what we want to

22   find out is how it's being used so that down the

23   road we can spot issues. It is an

24   information-gathering enterprise. It is not

25   designed at the end of the day, at the end of these

1   sessions, to come up with policy proposals.

2   We have no predisposition on this. My own

3   view, as some of you have heard me say before, is

4   that this kind of enterprise is what Congress had

5   in mind in 1914 when it created a Federal Trade

6   Commission. Not just law enforcement, but a group

7   that would try to work with the business community,

8   with consumers, and others, to understand new and

9   emerging dynamic trends in the economy.

10   That is what we've been about over the last

11   five or six years. We've tried to restore that

12   tradition, and I certainly feel that this workshop

13   moves in that direction.

14   We have a wide variety of people here today

15   who represent the business community, the consumer

16   community, academics, and others, and if history is

17   any guide, we will at the end of the day have

18   learned a good deal from each other.

19   With that, we'll receive some words on

20   video from my colleague, Mozelle Thompson, but

21   while that's being set up, let me introduce my

22   colleague and friend, Commissioner Orson Swindle.

23   COMMISSIONER SWINDLE: Thank you very much,

24   Chairman Pitofsky. I would like to welcome you all

25   here, and before I forget it, the last couple of

7

1   days in preparation for this, Bruce Jennings and

2   his crew of youngsters around here have been

3   scurrying in about 9,000 different directions

4   making all this come together. Wires have been

5   dragged all over the building and I think we've got

6   a good set-up here, and this will be recorded for

7   posterity and hopefully there won't be too much

8   blood on the floor when it's all over, but it's a

9   delight to see you all.

10   I know so many of the organizations that

11   are represented here, you have a vital interest in

12   this, certainly from a personal perspective of your

13   business, but we are all, as the chairman says,

14   grasping to understand. And I would hope that we

15   would view this process here today, as we have in

16   previous workshops, as the Chairman mentioned, as a

17   learning process in which we listen and offer our

18   suggestions from time to time, but mostly we listen

19   to you, the practitioners, and try to get a better

20   understanding of what we're all about and what

21   we're doing here with this very controversial -- is

22   that a good word to describe it -- but the issue of

23   information flow and its effects and the concerns

24   that various and sundry people have today in the

25   consumer population or in business population.

8

 1   I do want to welcome you all here today.

 2   The use of third party information from public

 3   records, information aggregators and even

 4   competitors for marketing has become a major

 5   facilitator of our retail economy.

 6   Even Chairman Greenspan suggested here some

 7   time ago that it's something on the order of the

 8   life blood, the free flow of information. This was

 9   made even more clearly by a new study released

10   yesterday by the Privacy Leadership Initiative and

11   the ISEC Council of the DMA.

12   The study made it clear that consumer

13   prices would increase if public policy

14   significantly limited the flow of data into catalog

15   marketing and sales. At the same time, the digital

16   revolution, both online and offline, has given an

17   enormous capacity to the acts of collecting and

18   transmitting and flowing of information, unlike

19   anything we've ever seen in our lifetimes.

20   Obviously the debate has been furious over

21   the appropriateness of these data flows, this

22   passage of information from one entity to another.

23   The perceived harm that this data flow

24   causes and what the appropriate remedies might be.

25   As we all know, we've had a heavy debate on privacy

1   going on now for at least three years, I've been

2   here three years, and it was going on even before I

3   arrived.

4   I believe that issues related to the real

5   harm that might be caused are well addressed by

6   existing laws, but now we need to explore issues

7   related to customer or consumer and business

8   entities or the seller and the buyer, if you will.

9   It is also useful to note that the digital

10   revolution has revolutionized the knowledge that

11   the buyer has about the marketplace. Buyers today

12   are more informed than they have ever been ever

13   before. The information age and information

14   technology is literally changing the way every one

15   of us does business, the way we conduct our lives,

16   how we pick and choose, and certainly this

17   information flow has made the buyer far more

18   informed.

19   It is crystal clear that there have been

20   quantitative and qualitative changes in the

21   marketplace, and the manner in which information is

22   made available and used.

23   There are real benefits in this for both

24   consumers and businesses, from these changes.

25   There are also changes in the way we all interact

```
 1    with each other.  More of the interaction is being

 2    defined by data and less by each of us based on

 3    what we reveal about ourselves.

 4         The FTC has traditionally dealt with harm

 5    that comes from bad actors and market failures.

 6    The issues being raised today don't necessarily

 7    fall easily into either of those categories.  Such

 8    as the challenge that we face.

 9         Productivity gains are well documented and

10    the new technology, as I said earlier, is changing

11    the way we do everything.  However, there is a

12    great trust deficit in existence out there now.

13    The public has concerns about the private sector's

14    ability to govern information use, or manage that

15    information that they happen to have on people.  At

16    the same time, the same observations will tell you

17    that the public has great concern as to what the

18    government does with the information it has.

19         And I would contend that we might ought to

20    be a little bit more concerned about what the

21    government is doing than the private sector, but

22    nevertheless, we've got a great distrust going here

23    between the consumers who more and more today

24    understand the value of their information, and what

25    goes on around them.
```

11

1   We therefore have a dilemma. The use of

2   information drives our economy, I think that's

3   pretty well established. That includes information

4   to make sales, marketing and customer service more

5   efficient, and more effective. The information

6   flow allows businesses to build the right product,

7   deliver it at the right time, to the right place,

8   to the right address, and meet the demands, unique

9   as they are, among all consumers, carefully

10   tailored to them. That I would suggest most

11   consumers would say not a bad deal.

12   However, this increased use of information

13   about people creates consumer concerns. The public

14   is concerned about the potential misuse of the

15   information, and individuals are concerned about

16   being defined by the existing data on themselves.

17   This is a huge misunderstanding deficit

18   that parallels and matches the trust deficit.

19   Consumer education has lagged market changes driven

20   by new technology. Government is behind the new

21   technology changes, too, as we've all noted.

22   Consumers struggle to understand the

23   technology itself, not just in the ways in which a

24   technology is used in the marketplace, I'm still

25   wrestling with my ISP, I was about to use a name

1   there, but I won't. I'm having so much trouble

2   with it, I don't want to defame the country at this

3   point in time, but I'm having trouble with the

4   technology itself, not to mention the information

5   flow.

6   Today's workshop is a great opportunity to

7   begin to bridge this learning gap and this trust

8   and misunderstanding or untrust and understanding

9   deficit. We're here today to gather facts and

10   begin to understand the flows of data that support

11   marketing and customer service.

12   This should increase our understanding of

13   the benefits of the free flow of information, and

14   to begin to understand the level of real harm, to

15   whatever degree it might exist, related to

16   information use.

17   And perhaps we have an opportunity to ease

18   the fears that are related to that emotion of fear

19   of the unknown. I would suggest, plead with,

20   counsel all participants to please leave your

21   emotions at the doorway.

22   This session today, folks, please, is not

23   about sound bites, it's not about exposing people

24   in public, it is about learning and sharing what we

25   each know and how we go about doing what we are

13

1   concerned with, and understanding how to balance

2   legitimate privacy concerns and economic and social

3   benefits.

4   Remember, today's objective is to learn, to

5   explore, and perhaps start to identify so we can

6   put our hands on it, some policy approaches that

7   are balanced in their -- they're balanced in a

8   sense that they balance the consumer's interest in

9   choice and economic opportunity, they balance the

10   consumer's interest in not being harmed by security

11   breaches and data misuse, they're balanced in the

12   sense that they respect the consumer's interest in

13   choosing when to not participate in a market, and

14   also the other side of the coin, so to speak, is

15   business interest in serving all markets in a most

16   effective and efficient and, quite frankly,

17   profitable way that they can. That's what you are

18   our free enterprise system is all about.

19   I thank you again for joining us. This is

20   an important session. Perhaps it's the first of

21   several important sessions on the very subject,

22   because I think we have a lot to learn and we

23   appreciate you coming here and being a part of our

24   family and helping us learn more, learn faster, and

25   hopefully, as I always say, helping us to look

14

1   before we leap. Thank you very much.

2   (Applause.)

3   COMMISSIONER THOMPSON: Good morning. I

4   would like to join the Chairman in welcoming you to

5   the FTC for this important workshop on the

6   Information Market Place.

7   As he mentioned, today we will all be

8   sharing what we know about the topic of Merging and

9   Exchanging Consumer Data. It's no secret, for

10   example, that the Federal Trade Commission has been

11   long talking about issues dealing with personal

12   data and privacy.

13   I think that today we will be talking about

14   how the issues raised with data collection converge

15   when we're talking about an online and offline

16   environment.

17   At present, there are some real reasons to

18   distinguish those two classes of information, in

19   light of the speed and the manner in which

20   information is collected. But I also recognize

21   that, as a practical matter, it doesn't make sense

22   for consumers and businesses to view separate

23   protocols for online and offline data collection.

24   So, I would encourage industry and

25   consumers to work together to formulate practical

1   solutions that foster consumer confidence.

2   But there will also be some important other

3   questions that you'll be dealing with today about

4   issues like legacy data, information that was

5   collected before there was an online environment,

6   and, also, how information changes -- does the

7   character really change when you have offline data,

8   including public information that's merged with

9   online data and made available in a mode like on

10   the internet.

11   I look forward to hearing your

12   presentations and hope that you'll enjoy the day.

13   Thank you very much for coming.

14   MR. WINSTON: Before we get started, I have

15   a few ground rules and announcements to make. The

16   first one I approach a little bit gingerly, but I

17   have been asked to ask all of you to turn off your

18   cell phones. I'm just the bearer of bad tidings

19   here. Apparently there's some feedback between the

20   cell phones and our equipment, and it's messing

21   everything up, so if you could please turn off your

22   cell phones.

23   Also, I would like to remind our panelists

24   that because we have so much ground to cover today,

25   we're going to try to hold you to the time limits

1   that we've discussed with you previously. We're

2   going to give you a one-minute warning before your

3   time elapses, and then when your time is up, we're

4   going to gently encourage you to conclude your

5   remarks. If that doesn't work, we have someone

6   with a hook who's going to come out and kind of

7   pull you away, but if you could try to stay within

8   the time limits.

9   Also, it's our practice in our workshops to

10   invite the audience to ask questions of the

11   panelists, if time permits, at the end of each

12   panel. But, again, because we have so much ground

13   to cover, I'm going to ask the questioners to limit

14   themselves to asking questions and not to make any

15   statements for the record.

16   Which brings me to my last announcement,

17   and that is that the record of this workshop is

18   going to remain open for 30 days, until April 13th,

19   so that anyone who wants to file something, a

20   comment or other materials, for the record, and for

21   the Commission's consideration, can do so. The

22   instructions for filing these post workshop

23   comments are available on our website at

24   www.ftc.org. So, I encourage you all of you to

25   participate in that process. Dotgov, I'm sorry,

17

1   somebody gave me the wrong web address here, okay.

2   Anyway, I encourage you all to submit comments if

3   you like.

4   Now we're ready for our first panel, in

5   which Professor Mary Culnan of Bentley College will

6   lead a discussion designed to provide an overview

7   of the flow of data through the information

8   marketplace. Professor Culnan is the Slade

9   Professor of Management and Information Technology

10   at Bentley College in Waltham, Massachusetts, where

11   she teaches and conducts research on information

12   privacy. She is the author of the 1999 Georgetown

13   Internet Privacy Policy Survey, and was a member of

14   the FTC's Advisory Committee on Access and

15   Security. And Professor Culnan will introduce the

16   members of her panel.

17

18

19

20

21

22

23

24

25

18

```
 1                    SESSION ONE:

 2          MERGER & EXCHANGE OF CONSUMER DATA:

 3                    AN OVERVIEW

 4          -   -   -   -   -   -   -   -

 5          MS. CULNAN:  Thank you, Joel, and thank

 6   you to the FTC for inviting me to participate in

 7   this workshop.  It's going to be a terrific day.

 8          One comment about our session.  We were

 9   instructed we're not going to have Q&A at the end

10   of our session, because we're just providing an

11   overview, so I didn't want you to think that we're

12   cutting off the flow of discussion arbitrarily.

13          What we are going to do today is we're

14   going to talk you through a slide, which I'm going

15   to put up here, and which you also have in your

16   packet.  Because the other two people are going to

17   be having their own slides.

18          We're going to talk you through this 30,000

19   foot view of profiling to set up the rest of the

20   day's sessions.  And so, if we skim over a topic

21   that you think we should have gone into in more

22   detail, you will hear about this in more detail in

23   the other sessions later on today.

24          We're going to focus primarily on the

25   compilers, the third party organizations that
```

19

```
 1    collect, slice and dice and then resell consumer

 2    data (but these firms do not have a direct

 3    relationship with consumers), rather than focusing

 4    on the profiling that's done by individual firms

 5    with their own customer data.

 6          And for the purpose of simplicity, we're

 7    also not going to talk about co-op databases, which

 8    fall into the category of third party organizations

 9    that collect information on customers, because

10    there's such a small number of these systems, but

11    for some of the things that we're going to talk

12    about, they also fall into our slide.

13          So, let me first introduce our two

14    panelists.  First is Johnny Anderson, who is the

15    president and CEO of Hot Data, Incorporated.  He

16    has over 30 years of technology industry

17    experience, holding executive and management

18    positions at e2 Software Corporation, Saber

19    Software Corporation, Novell, Excelan and Digital

20    Equipment.

21          Our second speaker is Lynn Wunderman, who

22    is the President and CEO of I-Behavior,

23    Incorporated.  Prior to founding I-Behavior, she

24    was the founding partner of Wunderman, Sadh &

25    Associates, which is a consulting firm specializing
```

1   in information-based marketing services for both

2   consumers and B2B marketers in the financial

3   services, high-tech graphic arts, non-profit and

4   Internet industries, and President and Chief

5   Operating Officer of Marketing Information

6   Technologies, a company providing database services

7   for major Internet and Fortune 100 companies. She

8   currently serves on the Internet committee of the

9   board of directors of the Direct Marketing

10   Association.

11   So, what we've done, we've divided the

12   slides into thirds. I'm going to discuss the first

13   part which is on the left, this is the consumer

14   part where consumers generate information in our

15   daily lives that ends up in a compiler's database.

16   Johnny Anderson is going to discuss the middle part

17   of what goes on in the compiler's black box, and

18   Lynn is going to discuss the third part on the

19   right, how compiled data is used to generate offers

20   to consumers, both prospects and consumers.

21   And then as you can see, our picture begins

22   and ends with the consumer, which is an important

23   point I think.

24   After I attended my first DMA convention

25   and went through the exhibits, I came away

21

1   convinced that anything anybody does puts you on

2   somebody's mailing list or you end up as a record

3   in somebody's database. And the slide shows some

4   of the main ways that this can happen.

5   First of all, all of us generate a number

6   of public records, depending on the kinds of

7   activities we engage in. Some of these include

8   personally identifiable information such as

9   property records, which do have our name and

10   address attached to them, or telephone directories

11   or other directories, and then there's public

12   records that have nonpersonally identifiable

13   information in them such as census records.

14   And compilers can acquire this information

15   in two ways. First they can acquire it directly

16   from the source, so they could buy the records from

17   the state or local government. Or they may acquire

18   the information from a second firm, such as

19   Claritas, that acquires this information and does

20   some analytics on it and then generates geographic

21   and demographic profiles that do not include

22   personally identifiable information but can be

23   overlaid on top of a record that does have an

24   address.

25   And in fact there was an example of this

22

1 information in yesterday's Washington Post, if you

2 happened to see this, of talking about Fairfax

3 County, Virginia that has the highest average

4 family income in the United States. And inside the

5 article, they talked about the different lifestyle

6 segmentation profiles that are represented by the

7 people who live in Fairfax County.

8   For example, they said 22 percent of the

9 people who live in Fairfax County are in The

10 Winner's Circle, that's the name of the profile, or

11 Executive Suburban Families, age 35 to 64,

12 household income is $90,700 a year, and these

13 people are most likely to have a passport, shop at

14 Ann Taylor and read Epicurean Magazine.

15   So, this will give you a flavor of how this

16 information is used to, again, help companies

17 understand who their customers or their prospective

18 customers are.

19   A second source of information is surveys,

20 such as warranty cards or marketing surveys that

21 could include questions about what people's product

22 preferences are across a whole range of different

23 kinds of products, their life styles, their

24 hobbies, and their demographics.

25   The third way that the information can end

23

1   up in a compiler's database is that people sign up

2   for mailing lists, and I was thinking about this as

3   I read the Sunday paper and, you know, there are

4   cards that fall out of the Sunday magazine where

5   you can request information on various topics.

6   Or people who order things by mail, or you

7   request information, call an 800 number, sign up

8   for something online, enter a sweepstakes or a

9   contest, and these types of things will put you on

10   a mailing list.

11   Well, mailing lists may be made available

12   directly, without going through a compiler, either

13   by the firm itself or more likely through a list

14   broker who is going to manage the mailing list on

15   behalf of the firm that owns the list. And that

16   can end up with targeted offers to prospective

17   customers.

18   Or some of the information may end up in

19   the compiler's database, and go into subsequent

20   uses that we'll hear about.

21   And then, finally, down at the bottom, we

22   see the customer database, and when consumers

23   establish a customer relationship with an

24   organization, with a business, they end up in the

25   customer database. And I think this is not a big

1   surprise to everybody.

2   And then that firm can generate new

3   targeted offers to its current customers. I think

4   people expect this to happen, but we're also going

5   to hear how compilers can help these firms generate

6   new offers to their customers, better target these

7   offers and help these firms do cross marketing of

8   new products and services.

9   So now Johnny will talk about what goes on

10   in the middle of the picture.

11   MR. ANDERSON: Good morning. My name is

12   Johnny Anderson, I'm Chief Executive at Hot Data.

13   How Data is an infomediary that connects customer

14   relationship management marketing automation

15   systems to sources of both household information on

16   consumers, and business information about

17   businesses, and provides a complete set of data

18   quality and standardization services for both

19   small, medium and large-sized businesses.

20   I'm going to spend a little time and talk

21   about the kinds of information that's collected,

22   how it gets compiled into a database, and then gets

23   delivered into a marketer's, end user's, database.

24   But first I want to kind of digress. I've

25   looked at some of the other slide shows, and a lot

25

```
 1    of the topics are going to be hit.  I really want

 2    to digress and talk about why people are -- why

 3    marketers are interested in this kind of

 4    information to begin with.

 5           Building a data warehouse and collecting

 6    this kind of information is a massive undertaking,

 7    and very expensive.  What's the payback, and what

 8    are businesses looking for out of taking third

 9    party information and merging that in with their

10    in-house information?

11           If you think about commerce, if you think

12    back, all the way back to the middle ages when

13    commerce really first started.  The buyers and

14    sellers knew each other.  There was a one-to-one

15    relationship.  Even up into the beginning of the

16    last century, people knew -- the storekeepers knew

17    who their customers were.

18           After World War II and the mobilization of

19    America, and the move from urban centers into

20    suburban centers, and the creation of the now

21    shopping mall, merchants now lost track of who

22    their customers are.  They don't know who buys

23    products anymore.

24           So, merchants really spend a lot of time

25    doing product level analysis to figure out who
```

26

1   bought the stinky cheese, and what stinky cheese

2   purchases drove what other kind of purchases.

3   The change in the new economy, and the

4   evolution of the Internet now has really empowered

5   consumers with information, and has broken down a

6   lot of the geographic boundaries in terms of, I

7   have to travel to a mall to purchase something.

8   This has already been broken down quite a

9   bit with the direct marketing and catalog

10   industries, but now with the Internet, people now

11   have a lot of information.

12   So, it is now dependent on -- a business'

13   dependence on success is now leveraged by what kind

14   of service they can deliver. And to deliver that

15   service, they again have to know who their

16   customers are.

17   So, you really look at all of the kinds of

18   information that's available so that businesses can

19   get a complete 360-degree view of their customers

20   to be able to understand them not only in the

21   context of their own transaction that may have

22   taken place, but also what the likes and dislikes

23   of that customer are.

24   So, when you really look at the kind of

25   information that's available, it really falls down

1   into three categories. There's the geographic

2   information, or where you live, and that kind of

3   information is really address data, quality of the

4   address, standardized to the Post Office's

5   standards, what's the bar code for the address, but

6   also includes information like what MSA that

7   address is in, what census tract that address is

8   in, and important things like latitude, longitude

9   and geocoding, which are really used by businesses

10   to do things like drive time analysis, and trade

11   area analysis.

12   But one of the first segmentations, at

13   least in the retail industries, and now in the

14   telecom industries, is where do you -- where do

15   people live and how far are they likely to travel

16   to get to one of my retail locations.

17   The second is really the demographic

18   information, and the collection and the detail of

19   this will really be talked about a lot in panel

20   number 2, but that's things like name, address and

21   phone number, at a very basic level, but also

22   reported and modeled information around a person's

23   income level, what their marital status is, whether

24   they buy by mail, whether they're a credit card

25   user, whether they own their own home or not,

28

1   information about what you're like.

2   And then the third piece is really the

3   psychographic information, and that's really what

4   you like, what your life style indicators are, and

5   that's where a lot of the compiled information

6   comes in from, lists and surveys, to determine what

7   somebody's propensity to buy a specific kind of

8   product is. And those are indicators that could be

9   that you're an outdoors enthusiast, a gardening

10   book reader, dot, dot, dot, there are a number of

11   different life style indicators.

12   So, how is that information merged into one

13   particular database? Data compilers really look to

14   those three sources and do a very complex job of

15   extraction, transformation and loading of that

16   data. And that data is bought from public sources,

17   and that could be things like tax records, home

18   owner information, up until recently motor vehicle

19   information was used, and in some states, even

20   driver's license information.

21   But that information is reported

22   information that's public record that's brought

23   into the database. Self reported data really

24   drives a lot of the demographic and psychographics,

25   and that's information from surveys and warranty

1   cards and registrations.

2   And then information from mail lists, and

3   that is I'm -- I have a wooden boat, I subscribe to

4   Wooden Boat Magazine. If I subscribe to Wooden

5   Boat Magazine, there is a great likelihood that I

6   am likely to buy products for wooden boats.

7   So, affinity modeling and propensity

8   scoring is really driven by the self-reported data

9   from both subscriptions and product registrations.

10   That information is matched based on name

11   and address, so that there's really a view of a

12   consumer that takes into account all of those

13   different kinds of data sources. And then there's

14   some additional modeling that's done on top of

15   that, based on scientific samples and surveys,

16   different kinds of models are put into place for

17   specific vertical industries.

18   Not every industry is interested in the

19   same kind of consumer information. A telecom

20   merchant is not interested in the same kind of

21   information that a retailer is interested in.

22   So, modeling is done based on a set of

23   attributes that's been collected to be able to put

24   together things for financial services and other

25   industries. And then the output of that

1   information really goes to two sources.

2   One is the data enhancement source, in that

3   I have a customer database of people that have come

4   to my company from a number of different sources,

5   could be a customer that signed up for a frequent

6   buyer program at a retail location, could be a

7   customer that's come to me at a trade show or sent

8   back a business reply card, or a customer that's

9   walked into one of my retail locations.

10   The customer that's in my database, so I'm

11   really looking for information that's outside my

12   organization so I can understand that customer

13   better.

14   And the second is the targeted lists, and

15   that is really if I've done some analysis in terms

16   of what my best customer looks like, give me some

17   more prospects that I can market that look just

18   like those folks. I don't know who they are yet,

19   and in most cases those targeted lists are going to

20   go to a mail house who is going to get a mail drop,

21   and I won't know who they are, until they respond

22   to that direct mail campaign and come back into my

23   database.

24   And then they'll go into the normal process

25   of my selling process inside my customer database.

 1   So, there will be a lot of detailed talk

 2   about both the collection of data in the second

 3   panel, and then the use and kind of how the

 4   technology drives some of the business models for

 5   the use of that data in the third panel a little

 6   bit later on.

 7   So, with that, let me turn it over to Lynn,

 8   and let her talk about some of the internal uses of

 9   data.

10   MS. CULNAN: Thank you, Johnny.

11   MS. WUNDERMAN: Bear with me just one

12   second here. Thank you.

13   Well, I've been asked to spend the next 15

14   minutes talking to you about the end user

15   applications that have evolved really over the last

16   two to three decades, so it might be a little

17   tight, but we're going to do the best we can.

18   I'm going to start where Johnny left off,

19   which is to help you understand how this kind of

20   compiled data really brings a name and address

21   record to life for a marketer.

22   Now, this is a real, live consumer record

23   off of a compiled database. I can attest to it

24   because it's me, it's the Wunderman household at 94

25   Mercer Avenue in Hartsdale, New York. I have

1   signed a release so that my data can be made public

2   here today. But just from that information, we can

3   now geocode this record and find out its census

4   block group, attach all the geographic information

5   available for the census, as well as we can now

6   construct a match code, which you see here on the

7   right side of the screen. That match code is the

8   link to the compiled database by which we overlay

9   the demographic and the psychographic information

10   that Johnny was just earlier describing to you.

11   Now, what happens when we do that? This is

12   pretty much what you get, on the Wunderman

13   household, a fairly distinct profile of a

14   relatively affluent middle-aged, suburban couple,

15   dotes on their dog, is extremely mail responsive,

16   somewhat techno savvy and lives pretty much a

17   high-end, fairly active life style.

18   Now, I can tell you this is a pretty

19   accurate record. There are two things they missed

20   here. They missed the registration on my husband's

21   antique motorcycle, okay. They are off by one

22   category on our income; that's okay with me if it's

23   okay with the IRS.

24   But why do we want this data? Why do we

25   want this information? As Johnny said before, it's

1   not because we're being nosy, it's because we're

2   looking to establish and build a relationship with

3   a consumer.

4   Now, Webster defines a relationship as a

5   connection, a bonding or a contract, and the way we

6   build relationships for marketing purposes is

7   really no different than the way we establish and

8   nurture relationships in real life. I mean, we do

9   it through data, whether it's by factual

10   information or observation, we're looking to

11   establish some common ground by which we can create

12   a meaningful, relevant communication to gain that

13   connection.

14   Now, I will tell you that the way it's done

15   by general advertisers is different from the way we

16   do it as direct marketers. In fact, it's the exact

17   opposite.

18   As a general advertiser, I'm looking for

19   large numbers of people with something in common.

20   Maybe I'm targeting women, 25 to 49, maybe some

21   broad-based income qualifier. I'm going to talk to

22   them based on what it is these women have in

23   common. Or at least I think they have in common.

24   Now, the issue is just because these are

25   women largely of child-bearing age doesn't

34

1   necessarily mean they have kids, but when I'm

2   spending $7 to $10 a thousand to reach them on TV

3   or maybe $20 to $30 a thousand to reach them in

4   print, I can afford to have a certain amount of

5   misses there.

6   But it's very different when you're a

7   direct marketer. I may be spending $500 or $1,000

8   a thousand to reach somebody at an individual or at

9   a household level.

10   So, I'm going to be much more stringent and

11   rigorous when I look at and evaluate the success of

12   that communication. I'm not looking for soft

13   measures like awareness or reach and frequency, I'm

14   looking for that household to take a specific

15   action, and I'm going to valuate the cost

16   efficiency of that action based on return on

17   investment.

18   So, I've got to be much more precise in my

19   ability to target that household and develop a

20   meaningful, relevant communication so I can capture

21   their attention and do it quickly.

22   So, we've learned over the years as direct

23   marketers a very important principle over the

24   years, and that is that people's differences are

25   more important than their similarities.

1   Now, what do I mean by that concept? I

2   mean that what it is when you're studying a group

3   that sets them apart from everybody else is more

4   important than what it is that the people in that

5   group have in common with each other.

6   So, the differences are more important than

7   their similarities, and they respond better when

8   those differences are recognized.

9   Now, here's what I mean by differences.

10   It's all the data we've been talking about. It

11   might be geographic, could be climate, market size,

12   it might be demographic, life stage or life stage

13   change, you know, maybe I just got a new spouse,

14   got a new house, got a new baby, preferably in that

15   order.

16   It could be psychographic information,

17   hobbies and interests we've been talking about, or

18   it could be your purchase history. Now, we haven't

19   talked a lot about that, but that purchase history

20   could be self reported that I got off of some kind

21   of a survey, or it could be the purchase history

22   that a marketer captures and utilizes in their own

23   database.

24   And normally when we talk about this, we

25   talk about the recency, the frequency, the monetary

36

1   value segments as a marketer. And I will tell you

2   this is incredibly powerful information from a

3   segmentation standpoint.

4   So, I might talk to you differently if

5   you're a new customer versus a tenured customer.

6   I'll not only talk to you differently, but I'll

7   invest differentially if you're a high-value versus

8   a low-value customer, and I'll have an entirely

9   different contact strategy, frequency of the kind

10   of offers I'm going to send you, if I happen to

11   know that you're a loyal customer as opposed to a

12   competitive switcher.

13   Now, as I said, this behavioral information

14   is incredibly important to marketers, and it works

15   terrificly, if you have it. But you don't always

16   have it. I mean, it's great if I'm talking to a

17   group of customers that have been with me a long

18   time and I have a lot of data on those people, it's

19   an established product, it's a proven offer, but

20   what do I do in a situation when I'm trying to

21   attract new prospects into the base? I don't have

22   a lot of data about their purchase behavior,

23   particularly about what they're buying from my

24   competitors.

25   What about if I'm trying to spend on my new

37

1   customers based on their potential to become

2   high-value customers every time. Not much there in

3   my database about these people. Or if I've got

4   some test market results that I've done with new

5   offers, new products, I know in aggregate how

6   people are likely to respond, but I've got to think

7   about who do I target with those offers because I

8   don't have that response information on everybody

9   in my database.

10   So, what do we do? We use surrogate data.

11   We use surrogate data as a bridge to help us be

12   able to apply that behavioral information to

13   another universe.

14   Now, the most important data that we tend

15   to use as surrogates is this compiled information

16   we're talking about today, because there's a very

17   important criterion that data has to be as

18   available on the target audience that I'm studying

19   as the application universe that I'm applying it

20   to. And the compiled data is virtually available

21   on just about every household in the U.S.

22   So, what I am going to do is I am going to

23   use my behavioral data in my own customer database

24   to define a target. I'm then going to use the

25   bridge data, the compiled data to describe the

38

1   target and create a profile, and then I'm going to

2   use that profile to help me find lookalikes in some

3   larger application base.

4   So, let me show you schematically how this

5   works. I'm a marketer and I have defined a target

6   as my high-value customers, however I define it,

7   profits, revenues, purchase frequency, et cetera.

8   And my goal is that I'm looking to identify

9   prospects in the population who have a high

10   potential to become high-value customers every

11   time, I want to track them into my base.

12   So what do I do? I'm going to study how do

13   these high-value buyers look different from

14   everybody else in the U.S.? And the data I'm going

15   to use to do that is all the demographic

16   information, the psychographic information, and I

17   will tell you the coverage on the psychographics

18   does not tend to be as large as some of the other

19   data, so it doesn't often enter these statistical

20   analyses, but we use it and we see if it's

21   predictive. The geographic data and the census

22   information, all to help me understand what is it

23   about this group that makes it look different from

24   everybody else.

25   I'm going to overlay statistical tools so

1   that I can really quantify which of these

2   differences are statistically significant in

3   identifying this target. I'm going to look at the

4   interaction and the relative weight or strength of

5   those variables, and I'm going to apply it back to

6   a broader universe, in this case, the U.S.

7   population.

8   Every household gets this -- every

9   household gets a score, excuse me, and the highest

10   scores are the most likely to generate and to

11   exhibit that target behavior. Those at the bottom

12   are least likely to become your high-value

13   customer, and this is nothing more than a planning

14   tool. Okay, I'm going to penetrate that universe

15   of U.S. population based on my volume objectives,

16   my budget limitations, whatever.

17   Now, I think it's important for you to

18   understand as we talk about these concepts, where

19   the predictive value of that data comes from.

20   Okay, and I promise, no formulas, you don't need to

21   be -- have a degree in applied statistics, it's a

22   very simplistic example.

23   I'm just going to use marital status and

24   I'm only going to give it two values. So, here I

25   am studying my high value-customers, all right, and

40

1   I'm looking at them and I see well, big deal,

2   they're just as likely to be married as they are to

3   be single, that doesn't tell me much of anything,

4   does it? How do I target anything based on this

5   information, how do I talk to them based on this

6   data?

7   Well, guess what? I compared them to the

8   U.S. population, and they're twice as likely to be

9   single as the rest of the population at large.

10   Now, take this predictive value, multiply it times

11   another half dozen to a dozen variables, you start

12   to see where the power of these statistical tools

13   comes from.

14   So, how do we use these tools? Well, we

15   use them to help drive differential contact

16   strategies. Who do we target, when do we target

17   them, how do we target them so that we're more

18   efficiently reaching them with more relevant

19   communications across the entire life cycle of the

20   customer. From acquisition to value stimulation,

21   all the way to eventual retention and

22   re-activation.

23   So, for instance, I'm going to rank my

24   customer database based on this information, and

25   I'm going to spend differentially based on the

1   probability of these people being high-value

2   customers, the repeat sales, cost sale, up sale,

3   I'm also going to apply it as well to my customer

4   information applications. Maybe I'm even going to

5   develop new services for high priority customers.

6   I can overlay this data on any vertical or

7   apply it out from a compiled database, I can use

8   this for direct sale or regeneration offers. Also

9   remember, that because this tool is developed at an

10   individual household level, I can aggregate it back

11   up to any level of geography.

12   So, for local support programs where

13   there's a retail trading area or there's a sales

14   territory, it become a very useful tool to

15   prioritize differential media and households for

16   these purposes.

17   It's easy to apply them to any form of

18   addressable media, those that are available today,

19   such as selective binding, addressable cable and

20   satellite, some of the Internet applications you

21   can hear about later this afternoon, and those

22   that, you know, we've hardly thought about in the

23   future, wireless, interactive television and things

24   that haven't even been invented yet today.

25   And these tools can also be used as a

42

 1   planning template, we can bridge them into

 2   syndicated research bases, such as Scarborough,

 3   MRI, Simmons, Nielsen, and help us optimize the

 4   value of our mass media, of our print and our

 5   broadcast spending.

 6   So, all of this is based on our study of a

 7   high potential end user.

 8   So, what does this do for us in the end? I

 9   mean, basically it helps marketers invest their

10   marketing dollars smarter, more efficiently

11   reaching customers across virtually every channel,

12   and for consumers, it means hopefully you receive

13   more of the offers you want, and fewer of the

14   offers that you don't. And that to us is a win-win

15   for everybody. Thank you.

16   MS. CULNAN: We've got a lot of time left,

17   we've got about 25 minutes. What would you like us

18   to do?

19   MS. ALLISON BROWN: Do you want to take

20   questions?

21   MS. CULNAN: Sure, we'll take questions.

22   We changed our minds, we'll take some questions.

23   And there's a microphone over here, so I think

24   Jason Catlett has a question.

25   And then if you would address your question

43

```
 1    to one of the panelists, if that's your preference,

 2    please do so.

 3              MR. CATLETT:  May I address it to you,

 4    ma'am?

 5              MS. CULNAN:  You may.

 6              MR. CATLIN:  Hello, this is called the

 7    bleeding edge of technology.  Well, I don't think

 8    it's doing anything, but I'm going to hold it here

 9    anyway.

10              Mary, you said that you were not going to

11    address co-op databases on the basis that there are

12    so few of them.  And I think that's like saying

13    we're not going to address suppliers of Windows

14    operating systems because there are so few of them.

15    The dominant co-op database, Abacus Direct, really

16    has enormous influence, and I think it's a model

17    different to but very relevant here.

18              So, could you take a minute to describe

19    what co-op databases do?

20              MS. CULNAN:  I may punt this to one of the

21    panelists who have more experience.  I will say one

22    thing, for those people that are interested in

23    co-op databases, and particularly in Abacus Direct,

24    their data dictionary is on the DoubleClick

25    website, so if you go to doubleclick.com and you
```

44

1   click on Abacus, you can see exactly what kind of

2   information they have acquired, and I think

3   probably it's a really good example of

4   transparency, assuming you know to go there and

5   look for the data.

6   So, because Lynn is actually running a

7   co-op database, and again, it's not that we didn't

8   want to talk about these because we didn't want to

9   hide anything, but because we were doing the broad

10   overview, we decided as a panel it would confuse

11   things, thinking our talks would take longer if we

12   went off and then couldn't fit it all into the

13   slide.

14   MS. WUNDERMAN: I do promise that we will

15   spend some time this afternoon talking about the

16   co-op database model, and specifically about my

17   company, I-Behavior, unless there's something

18   specific to these applications that you would like

19   to talk about now.

20   I mean, I could go into the concept of

21   co-op database, it's going to be a little redundant

22   this afternoon.

23   MR. CATLETT: Why don't you spend 30

24   seconds describing a co-op database.

25   MS. WUNDERMAN: A co-op database is formed

45

1   when marketers share their customer names and

2   related buying information in order to gain access

3   to names of qualified prospects as well as

4   additional data on their customers that might

5   otherwise be unavailable for them to market and to

6   build their business.

7   So, if we had, I don't know, Mary, if you

8   could put back your first slide.

9   MS. CULNAN: Sure.

10   MS. WUNDERMAN: I mean, basically with a

11   co-op database, if we move the consumer aside to

12   the right and we were to create another box, what

13   you would see is the customer databases, the

14   compiled data would all come into a co-op database

15   and we would have a consolidation of many customer

16   files from marketers, publishers, catalogers,

17   e-tailers, et cetera, all going into one database

18   as well as it would be overlaid with the

19   demographic or the psychographic as well as the

20   census data we've been talking about earlier, all

21   to form a positive record. And that is the rich

22   behavioral and demographic base upon which

23   marketers would be able to do selections from that

24   file.

25   MR. CATLETT: Thank you.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025

46

1   MS. CULNAN: One difference I think it's

2   important to point out, you have to be a partner in

3   the co-op database.

4   MS. WUNDERMAN: Yes, you do.

5   MS. CULNAN: You have to put data in in

6   order to take advantage of the data that's there,

7   as opposed to the compiled databases where

8   basically there's no relationship between

9   contributing data to the database and being able to

10   acquire data from the compiler.

11   MS. WUNDERMAN: Yes, and I will also say

12   that generally that there's notification to the

13   consumer about sharing data with trusted third

14   parties as well as the online component, there are

15   privacy protections as well.

16   MS. CULNAN: Anybody else? There's a

17   question toward the back.

18   MR. TUROW: Would you talk just a little

19   bit about the way databases get purged, based not

20   just on what consumers want, but also recency and

21   the decision that certain things become obsolete

22   and how those criteria are determined?

23   MS. WUNDERMAN: I want to make sure that I

24   understand your question. You're asking, you know,

25   I think on -- in terms of if I have information in

47

1   a customer database about an individual's purchase

2   behavior and over time that that data is no longer

3   relevant? Is that --

4   MR. TUROW: Yeah, how do you decide -- how

5   do you decide at what point you purge those

6   particular data like your sports car. Maybe you

7   decided to get more conservative about the car and

8   somebody has not picked it up, do you have any kind

9   of criteria to which to purge certain kinds of data

10   after a certain amount of time, based on certain

11   other criteria?

12   MS. WUNDERMAN: Let me say something about

13   the compiled data and its value, because they're

14   not going to be always 100 percent accurate. I

15   mean, you saw even my income on my own personal

16   record was not accurate. What's of greatest value

17   with the compiled data beyond its coverage is its

18   consistency, and when you're looking for predictive

19   value, consistency can be even more important than

20   sheer accuracy.

21   So, the procedures that are in place to

22   replace that information, the models that are done

23   to calculate data such as income, it's consistently

24   done even if it's inconsistent across households.

25   So that as that data is predictive, it may be

48

1   predictive, even though it's not 100 percent

2   accurate, but if it is predictive, it will rise to

3   the top, and then virtually it's a numbers game.

4   You will never be 100 percent on any

5   particular individual or household. What you're

6   trying to do is increase the probability of

7   identifying a high potential consumer.

8   So, for one or two or, you know, any number

9   of people, that data will still not be 100 percent

10   accurate, it ages over time, and it's the compilers

11   that capture that information from the various and

12   sundry public resources or surveys that gets

13   supplied back to us, it's accurate, it's not

14   accurate. But if it's still predictive, we will

15   still work with that information.

16   MR. SMITH: Richard Smith with Privacy

17   Foundation. I have a question for Lynn. How do I

18   get my compiled record, just like you got yours, on

19   the screen?

20   MS. WUNDERMAN: Call me.

21   MR. SMITH: Can everybody call you if they

22   want to see, every consumer if they want to see

23   this?

24   MS. WUNDERMAN: I'm sorry, you're asking

25   you as a consumer, how would you get access to

49

1   information? Well, I am not a data compiler, per

2   se, I mean we get our data from Equifax, there are

3   others, Experian, and First USA through their

4   Donelly unit and Acxiom through their InFobase that

5   supply this information, but if you as a consumer

6   are interested in seeing your record on our

7   database, you can request a copy of your profile

8   and we'll supply it.

9   MR. SMITH: Do these companies, compiler

10   companies generally allow consumers to look at this

11   kind of data?

12   MS. WUNDERMAN: You know, I --

13   not being a compiler. I would have to say in

14   today's marketing environment, they should, but I

15   cannot tell you. Certainly the data that comes,

16   for instance, from a credit bureau, and the credit

17   bureau information gets channeled as part of

18   Equifax and that gets channeled into the Polk

19   Database, as a credit bureau, you need to be able

20   to provide consumers with access to that data, but

21   I'm not familiar with the policies of each and

22   every compiler.

23   MR. SMITH: Thank you.

24   MS. CULNAN: Okay, I think we're going to

25   take a break and you want to break for -- you're

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025

50

1   going to let the people running this set the rules.

2   Thank you.

3   MR. WINSTON: This is kind of a unique

4   situation, we're actually ending a little early,

5   but that gives us a little more time for lunch.

6   So, if we could break until about 10:15, and I want

7   to thank the panelists and the Magazine Publishers

8   of America.

9   (Applause.)

10   MR. WINSTON: Also, thank you to the

11   Magazine Publishers of America for supplying our

12   repast out there.

13   (Pause in the proceedings.)

14

15

16

17

18

19

20

21

22

23

24

25

51

```
 1                        SESSION TWO

 2               CONSUMER DATA:  WHAT IS IT?

 3                   WHERE DOES IT COME FROM?

 4               -    -    -    -    -    -    -

 5               MS. ALLISON BROWN:  Hi, I'm Allison Brown,

 6    I'm an attorney in the FTC's Bureau of Consumer

 7    Protection, and I'll be the moderator for Session

 8    2, entitled Consumer Data:  What Is It?  Where Does

 9    It Come From?

10               The overview that we just heard has

11    provided us with a brief look at data merger and

12    exchange.  Now we will begin a series of in-depth

13    panel discussions about these practices.

14               This panel discussion will focus on the

15    original sources of consumer information, and we

16    have five very experienced and knowledgable

17    panelists with us today for the discussion.  We

18    will also have about ten minutes at the end of the

19    panel for the audience to ask questions.

20               If you're sitting in an overflow room and

21    you want to ask a question, please come up to the

22    doorway on the main room here on the fourth floor

23    at about 11:20 and we'll have a wireless microphone

24    here so that you will be able to ask the panelists

25    your questions.
```

52

1   I will now introduce each person on the

2   panel and ask the panelist to spend about three

3   minutes to provide a brief introduction to the

4   sources of consumer data that businesses use.

5   C. Win Billingsley is the Chief Privacy

6   Officer of Naviant, Inc. Naviant is a provider of

7   marketing tools and integration methodology for

8   online and offline environments.

9   Win, please go ahead with your introductory

10   remarks now and I'll introduce the other panelists

11   in turn.

12   MR. BILLINGSLEY: Okay. Naviant is a

13   leading provider of integrated precision marketing

14   tools, for both online and offline environments.

15   So, we really integrate the virtual world with the

16   physical world.

17   This capability enables marketers to

18   identify, reach and build relationships with online

19   consumers. So, to probably state that in a form

20   that is more meaningful to you, Naviant has a

21   database of about 30 million households that are

22   Internet-enabled.

23   So, our niche is a database of people who

24   have the capability to buy products and services on

25   the Internet. This data is collected primarily

1   through product registration data, and we'll talk a

2   little bit more about that in the session on how

3   this actually occurs.

4   The data is fully permissioned. We only

5   want people in our marketing database that

6   permission us to do so. You know, an individual or

7   an Internet user that does not want to participate

8   in Naviant's database is not included in the

9   database.

10   And then there are other processes that we

11   have in place to make sure that our data is

12   accurate and as useful as possible.

13   MS. ALLISON BROWN: Okay, Elisabeth Brown

14   is Senior Vice President of Product Strategy for

15   Claritas. Ms. Brown oversees the development of

16   new data products and services, including

17   demographic, cartographic and segmentation systems,

18   and the management of the software and applications

19   that are delivered to Claritas clients.

20   Ms. Brown?

21   MS. ELISABETH BROWN: Thank you. One

22   comment, too, I have actually been not only am I a

23   member of the club, but I have been a client, so I

24   was actually a client of the Claritas marketing

25   products and services before I joined the company.

54

1   So, I do have a little bit of perspective on how it

2   can be used and how we used it when I was at the

3   Prudential Insurance Company.

4   Claritas is a marketing information company

5   that has been in business for over 30 years, which

6   makes us one of the more mature companies in this

7   industry -- as evidenced by a recent Wall Street

8   Journal article that referred to Claritas as the

9   granddaddy of demographic providers.

10   Claritas serves companies in financial

11   services, telecommunications, energy, automotive,

12   retail, restaurant and real estate industries, and

13   we have clients ranging from the top Fortune 500

14   companies to small, independent consultants.

15   I'll just give you a little bit of

16   background. Over 30 years ago, Claritas' founder,

17   Jonathan Robbin, who was a Harvard social

18   scientist, was analyzing U.S. Census data and

19   settlement patterns. He hypothesized that American

20   neighborhoods reflected the old adage that birds of

21   a feather flock together, and therefore, the

22   products and services that Americans consumed could

23   be predicted simply by knowing summary level

24   demographic information about the area, or "you are

25   where you live."

55

1   This was referred to in the first slide as

2   geodemography. Thirty years later, our models have

3   become more sophisticated and are able to dissect

4   markets at a much lower level of geography, but

5   that same old basic premise still holds true that

6   by knowing some small amount of demographic

7   information, you can infer or predict the

8   likelihood that a household will be interested in

9   the products and services that you're offering.

10   So, we provide demographics and other

11   consumer and business data on multiple levels of

12   geography, delivered through our various mapping

13   and marketing application software platforms.

14   We are probably most well known for our

15   consumer segmentation systems, for example, Prism,

16   which was also identified earlier when Mary was

17   speaking about Winner's Circle and what some of the

18   attributes of a neighborhood would be that would be

19   tagged as Winner's Circle across the country. Our

20   consumer product demand estimates that our clients

21   use to more efficiently market their targeted

22   customers and prospects, which you could refer to

23   as surrogate or inferred data.

24   Claritas data and services are used for

25   broad marketing functions such as tracking new

56

1   customers, retaining current customers, determining

2   site locations and appropriate sales and marketing

3   distribution channels, and we help with more

4   efficient reach strategies and media planning.

5   So, basically, Claritas marketing

6   information helps our clients offer the right

7   products and services in the most appealing way to

8   the consumers and prospects. We provide basically

9   the benchmark information or the total universe

10   data that our customers can use to compare their

11   current customers and markets against so that they

12   can make better marketing decisions. Thank you.

13   MS. ALLISON BROWN: Next we have Paula

14   Bruening who is Staff Counsel for the Center for

15   Democracy and Technology. The Center for Democracy

16   and Technology is a non-profit public interest

17   organization that seeks practical solutions for

18   enhanced free expression and privacy in global

19   communications technologies.

20   MS. BRUENING: Thank you.

21   CDT has been asked today to discuss the

22   issue of public records as a source of information

23   about individuals from a factual basis, and as many

24   of you know, CDT generally has a specific viewpoint

25   on this issue. I will talk today about the factual

```
 1    basis in my opening remarks and then any other

 2    comments will be reserved for the Q&A, but I would

 3    like to encourage the FTC to go to the state level

 4    and to some other resources and some organizations

 5    that are doing work on this issue, because I think

 6    some of the really difficult work on how the

 7    information is collected and how it is being used

 8    specifically is being done at the state level.  And

 9    I'm happy to give the FTC that information.

10            Public records maintained by government

11    agencies disclose a vast array of detail about an

12    individual's life, activities and personal

13    characteristics.  At the federal level, most

14    personal information is not available to the

15    public, because of the privacy exemption in the

16    Freedom of Information Act and the Privacy Act of

17    1974.

18            However, bankruptcy records are an

19    important exception to this rule and are maintained

20    by the federal courts.  These records are a source

21    of detailed financial information, and the

22    sensitivity of that information has been recognized

23    by the Office of Management and Budget, which has

24    produced a study on this issue called Financial

25    Privacy in Bankruptcy:  A Case Study on Privacy in
```

58

1   Public and Judicial Records.

2   At the state and local level, however, the

3   types of records that are maintained are different,

4   and the laws and policies governing records yield

5   disparate acts and disclosure practices, but it is

6   possible to construct a detailed profile about an

7   individual from public records.

8   And while I will spare all of you the

9   exhaustive list of all the sources of information,

10   I'll name a few: Name and address information come

11   from voting records; land titles are a source of

12   home ownership information; property taxes can give

13   you assessed value of homes; birth and death

14   records give you information about an individual's

15   parents.

16   The list goes on, there are occupational

17   license records, motor vehicle records that can

18   tell you about an individual's make and model of an

19   automobile, voter registration gives you party

20   political affiliation, and hunting and fishing

21   licenses, boat and airplane licenses can give you

22   information about how a person likes to spend their

23   leisure time.

24   There may be considerably more information

25   available in public records about an individual who

59

1   has interacted with the courts as a criminal

2   defendant, as a plaintiff or defendant in a civil

3   litigation, in a divorce proceeding, as a juror, as

4   the beneficiary of a will.

5   Public access to government records serves

6   several important goals. Individuals need

7   government information to make political decisions

8   about government programs, legislative and

9   regulatory options, and candidates running for

10   office.

11   Government records also assure the

12   accountability of individuals as in the case of

13   business and real estate transactions. However,

14   it's important that public record information be

15   used for the reasons it was collected. This

16   information was not meant to be searchable in a

17   database, nor was it intended to be used in

18   marketing. And simply because there is a tradition

19   of collection of information, important decisions

20   need to be made on a case-by-case basis about the

21   appropriateness of access to public records and the

22   role of consumer choice.

23   MS. ALLISON BROWN: Thank you.

24   Michael Pashby is Executive Vice President

25   and General Manager for Magazine Publishers of

1   America where he has also served as Executive Vice

2   President of Consumer Marketing. Before joining

3   the MPA, Mr. Pashby was president and publisher of

4   Art and Antiques Magazine, vice president of

5   circulation and new product development for Gruner

6   + Jahr USA, and Managing Director of U.S.

7   Operations for Marshall Cavendish.

8   Michael?

9   MR. PASHBY: Thank you. That sounded

10   impressive.

11   MPA represents about 85 percent of the

12   consumer magazine -- dollar volume of the consumer

13   magazine industry in this country, and about 85

14   percent of all magazines are sold through the

15   mails, using direct mailing techniques or direct

16   marketing techniques of extremely varying

17   sophistication.

18   The use of credit cards in our industry is

19   extremely small, but is now growing. Our members

20   strongly agree that we must protect the privacy of

21   our readers, and I think our industry has done a

22   very good job over the years in balancing our

23   legitimate business interests and our consumers'

24   reasonable expectations of privacy.

25   Obviously we value our readers and we

61

1   wouldn't be in business without them, so our

2   industry is constantly looking for ways to improve

3   that service to our readers.

4   It's important to note that when our

5   readers ask us not to share information about them,

6   we don't. In the information section of most

7   magazines, the publisher discloses that the

8   subscription list may be rented to appropriate

9   businesses.

10   The magazine offers an address or toll free

11   number so that the reader can opt out. And many

12   magazines are taking advantage of the Internet to

13   inform consumers of their privacy policies, and

14   give consumers an additional opportunity to opt

15   out.

16   We're very careful with respect to the

17   customers, to the wishes of the customers who

18   choose to opt out. Generally when a consumer

19   requests that publishers not share information,

20   that publisher will not only remove the consumer

21   from their own internal rental lists, but will

22   refer the consumer to the DMA so that the consumer

23   can request to be on their nation-wide do-not-mail

24   list.

25   That said, magazines are very good sources

1   for consumer data. And the reason is very simple.

2   More than any other medium, the choice of which

3   magazines a consumer reads can tell a lot about a

4   person, what a person likes, and his or her

5   interests.

6   In enabling our readers to get information

7   about products and services that are of interest to

8   them, it is advantageous to everyone. Our readers

9   are given more choices, they get information about

10   products of their interest and life styles, and

11   most importantly they're not inundated with

12   advertisements for products they have no interest

13   in.

14   Businesses benefit because they can target

15   their advertising to consumers who are most likely

16   to be interested in their products, saving them

17   time and money. And for magazines, with a cost of

18   mailing now between 65 cents and a dollar per

19   piece, and that's before the Post Office applies

20   for its newest rate increase this June, the cost of

21   acquiring a consumer, when the response rates are

22   in the low single digits, and in a very competitive

23   market, is extremely expensive.

24   But sharing information only works if it's

25   beneficial to everyone. Our magazine subscriber

63

1   lists are our most important and valuable assets,

2   our readers do not want to get advertisements for

3   products they don't care about, so the magazine

4   industry is selective about letting advertisers use

5   their lists.

6   If a business intends to mail a

7   solicitation to a consumer, magazine staff review

8   that promotion to ensure its use is appropriate.

9   Most magazine publishers will not rent their list

10   to telemarketers because they have little control

11   over how the list is used, but if lists are rented,

12   we expect magazine staff to review the

13   telemarketing script.

14   And very importantly, the list is rented,

15   it's not sold. That means the advertiser can use

16   it only one time. And publishers, as a general

17   course, see their lists and track how that list is

18   used.

19   Thank you for inviting us again.

20   MS. ALLISON BROWN: Thank you.

21   Our final panelist is Ted Wham. Ted is the

22   President of Database Marketing for the Internet, a

23   sole proprietorship consulting practice. His

24   career has been concentrated in the direct and

25   database marketing industries, focusing most

1   recently on Internet-enabled marketing

2   applications.

3   Ted?

4   MR. WHAM: The benefit of having the last

5   name of Wham is that although I am always at the

6   end of the line, I always get to hear what

7   everybody says before me and tailor my comments to

8   help amplify on those areas as well.

9   Database Marketing is an independent

10   consultancy that consists of myself as an

11   independent business person working out of my home,

12   and billing my cat at very low billable rates, I

13   have had an opportunity to work with organizations

14   such as Viacom Division, Curriculum Corporation,

15   Hewlett Packard, I have worked with Cisco Systems

16   here recently, NCR and so forth, helping them

17   formulate Internet privacy strategies and also how

18   to use information about consumers for part of

19   their contact strategies.

20   In general, the information which is

21   available about consumers in the United States

22   starts from very gross aggregate levels, compiled

23   information which is largely demographic

24   information, and as Ms. Wunderman explained in the

25   session immediately before this one, to a lesser

1   extent psychographic information.

2   You move from that into information which

3   is available from a wide range of public records,

4   such as the ones that Ms. Bruening referred to, and

5   ones that I have personal experience with as being

6   on the receiving side of some of the solicitations

7   for there.

8   That's important because those public

9   records the consumer doesn't have much choice in

10   terms of their participation in those lists, it's

11   an obligatory process. If I want to vote, I have

12   to register to vote, and if I register to vote,

13   those public records are then going to be available

14   for purposes unrelated to my voting, and, you know,

15   that's kind of the way it is.

16   There is then a second tier, and that is

17   government supported monopolies, and those

18   monopolies are, because they're either a natural

19   monopoly such as the provision of your gas service

20   or your telephone service, and for instance white

21   pages, telephone white pages are a major source of

22   compiled list information, but there's also

23   government supported monopolies in the form of

24   patent protection and copyright protection, which

25   gives a form of a unique ability to sell a product.

66

1   So, for instance, if I want to operate with

2   a computer operating system called Windows, I have

3   to support the patent and copyright protections

4   available from Microsoft until those patents run

5   out, and I have to use that information and

6   Microsoft has that and has the opportunity to share

7   that information, if that is their business

8   practice to do so.

9   There is a whole range of different

10   products from drugs that you have to take to the

11   type of services that you buy and so forth, where

12   that government-mandated protection is there. For

13   monopolistic practice it serves a public good in

14   terms of inspiring innovation.

15   The last area is information which is in a

16   much more competitive area. I can go to any of a

17   number of different retailers to buy clothing, for

18   instance, and the retailers when I make that

19   purchase are going to collect various amounts of

20   information.

21   So, if I buy at Sears, that may be a

22   largely anonymous transaction, especially if I make

23   it in a cash basis. If I do it through a credit

24   card, they may have more information, and some

25   retailers through a traditional retail environment

1   such as Radio Shack actually will ask you for

2   information about your name and address, and

3   collect that information online.

4   Other businesses who run their business

5   model through a mail order process such as Lands

6   End and J. Crew and so forth become much, much more

7   adept at collecting very specific information about

8   you because what you've bought in the past becomes

9   most predictive about what you will buy in the

10   future. It's dramatically better than demographic

11   information, dramatically better than any

12   information you're going to get from public

13   records.

14   If I bought something from J. Crew in the

15   past, I will be better than any prospect that they

16   can find to buy stuff from them in the future.

17   But there's an opportunity for a consumer

18   to make a choice in those purchases on whether

19   they're going to choose retailer A versus retailer

20   B, and so there's an opportunity for control there.

21   So, in looking at this, I think it's

22   important to look at the spectrum of how that

23   information is collected in terms of the consumer's

24   ability to control the use of that information

25   downstream.

68

1   MS. ALLISON BROWN: Now that you've heard a

2   brief introduction to the sources of consumer data

3   that businesses use, I'm going to ask our panelists

4   some questions so that we can learn some more

5   specifics.

6   Win, what data elements does your business

7   collect about consumers and how do you collect the

8   information?

9   MR. BILLINGSLEY: Most of us have done a

10   product registration or a software application

11   registration, and it's very important for the

12   manufacturer of that product to get to know who

13   their end user customers are, because all of them

14   distribute their products and services through some

15   intermediary. So, they're really isolated from who

16   their end user customers are.

17   The way they try to solve that problem, and

18   also to provide customer support and service, is

19   through a registration process. So, Naviant

20   provides software that is used by companies that

21   manufacture computer hardware and software products

22   to facilitate that registration.

23   So, the data that we collect for the

24   company includes all the information that we've all

25   seen on those product registration forms, but the

69

1   only data that Naviant really uses that goes

2   forward into a marketing database is the name and

3   the address, and the fact that this is an

4   Internet-enabled household.

5   And that's really what we focus on and what

6   we collect. The other information is analyzed

7   statistically and then passed back to the

8   manufacturer, and they can use it for various

9   business purposes to know who their customers are.

10   So, name and address, and the fact that

11   this individual is Internet-enabled is key to

12   our -- that's where the cycle starts with Naviant.

13   MS. ALLISON BROWN: What other data

14   elements do businesses collect about consumers and

15   how are they collected? Anybody? You can just

16   either raise your hand or put your tent card on its

17   side? Ted?

18   MR. WHAM: Yeah, I forgot the tent card on

19   its side, I don't live in Washington, D.C. That's

20   a rule.

21   Businesses often times have an insatiable

22   demand for information. They would collect as much

23   information as the consumer will spend time to

24   provide for them. In fact, one of the services

25   that I provide to my consulting clients is that I

1   will get the question, How much can we ask on a

2   registration process or in a survey process or

3   through a purchasing application before the

4   consumer is finally going to go Aye, "I don't want

5   to do this anymore" and will bottom out of that,

6   and they will test that very aggressively and try

7   several different formats. If we ask this extra

8   question, what's going to happen here? If I format

9   this as a drop-down question instead of a radio

10   button, what happens here and so forth. They will

11   collect as much information as they can until they

12   reach a point where the collection of that

13   information degrades completion of the desired

14   task.

15   MS. ALLISON BROWN: Betsy?

16   MS. ELISABETH BROWN: One of the things

17   that I didn't go over specifically is that there

18   are lots of sources of public information out

19   there, including the U.S. Census data, which is

20   pretty hot right now since it's been recently

21   updated.

22   Many companies are trying to get at this

23   information because it's a very good source for

24   benchmark information to understand sort of the lay

25   of the land. And when we talk about benchmark

1   information, there's a lot of other domain

2   information, public domain information that is also

3   collected and used by businesses.

4   Just from my experience at Claritas and my

5   experience with some of these customers, they

6   really do use a variety of information for

7   different business purposes, and from what we've

8   seen, we -- at Claritas, we try to assist them by

9   updating the demographic information annually so

10   they do have these benchmarks and we use lots of

11   different input sources, including consumer surveys

12   that are out there, you may have heard of people

13   like Simmons Market Research Bureau, Mediamark,

14   Nielsen Net Ratings, Scarborough, all of these are

15   collected with consumer consent, they're pretty

16   much anonymized in terms of you never really know

17   who these individual consumers are. Basically that

18   data is used and compiled and turned into models

19   that really say if the person is in this

20   demographic characteristic, they have a higher

21   likelihood than average to do these behaviors.

22   Some of the magazine data is used that way

23   as well. You can either use the individual

24   registration data or pretty much the anonymized

25   version which gives you the, quote, profile.

72

1   So, there are many, many databases that

2   Claritas and other companies produce and put out

3   there, and the only way that information is linked

4   back to a customer record is through an inferred

5   modeling process, which either takes into account

6   what we believe their demographics to be, or

7   something as simple as the zip code or zip plus

8   four in which they live.

9   MS. ALLISON BROWN: And can you be a little

10   more specific about the types of information that

11   Claritas gets from surveys, you know, either

12   through Simmons or through its own surveys?

13   MS. ELISABETH BROWN: Depending on the

14   panel, Simmons and Mediamark Research have various

15   surveys that they put out there, some of them are

16   books of information that ask everything from how

17   much peanut butter do you eat a week, to what

18   brands do you prefer, what media you like, how

19   often do you spend in front of the television.

20   A.C. Nielsen actually captures specific

21   readership and views of which television programs

22   and what day parts in terms of which actual

23   physical programs you're watching. And a lot of

24   that data, again, it's all consumers are signing up

25   for these panels. That's the panel type of

73

1   research.

2   In addition, there's other types of

3   research which is more of the research where you're

4   calling up people on the telephone or just sending

5   them a direct mail package and asking them

6   something more specific about the financial

7   services that they're using, or the types of

8   Internet services they have and that type of

9   nature.

10   Once again, most of this data, what happens

11   is that all the data is collected at a household

12   level, but when it's modeled and analyzed, it's

13   analyzed in terms of demographic characteristics or

14   segmentation codes and not -- those people that

15   participate in the panel, that data is never used

16   for specific marketing purposes back to those

17   individuals.

18   MS. ALLISON BROWN: Thank you. Paula?

19   MS. BRUENING: Yes, I just wanted to talk a

20   little bit about business use of public record

21   information, and clearly the kinds of information

22   that I talked about in my opening remarks are

23   valuable to businesses in their marketing pursuits.

24   The problem comes with the fact that the

25   information has been given up by the individual, is

1   given up so that they can participate, as Ted Wham

2   said, in some very basic functions of life. They

3   want to drive a car, they want to buy a house.

4   They've had a baby. Someone's been born or died in

5   the family. Someone's received money in a will.

6   And I think that to say that Well, that's

7   being used for other purposes, and that's just the

8   way it is, I think is a -- is not a really very

9   thorough analysis. I think that if anything, what

10   the information age, computerization, will allow us

11   to do is give us an opportunity to re-examine those

12   uses to decide whether those are appropriate,

13   whether we can limit the access to that

14   information, to the -- to something closer to what

15   the initial collection was intended for.

16   MS. ALLISON BROWN: Are there currently any

17   restrictions on the use of public record data for

18   marketing? Anybody?

19   MR. WHAM: There's one large restriction

20   that I am familiar with and that is recently there

21   was legislation passed at the federal level which

22   gives consumers an opportunity to opt out of having

23   their information about their automobile

24   registration used for marketing purposes.

25   MS. BRUENING: That's opt in.

1   MR. WHAM: Opt in, opt out, excuse me,

2   okay. So, but it was very, very significant,

3   because prior to that legislation 46 of 50 states

4   made their consumer automobile registration

5   information available to the list rental

6   marketplace, and what type of car you own and drive

7   is extremely predictive of your household income.

8   It's one of the most predictive items.

9   And so if I wanted to drive a car in the

10   state of California, I didn't have any choice, that

11   information was going to make it into R. L. Polk's

12   database.

13   That's an example where there have been

14   some restrictions recently.

15   MS. ALLISON BROWN: Michael, I think you've

16   been wanting to say something?

17   MR. PASHBY: I was just going to say the

18   magazines themselves collect a relatively small

19   amount of information about their consumers. The

20   sort of information that they have is the date of

21   purchase, the source of purchase, whether it's by

22   the telephone or from a magazine previously bought,

23   whether it's through direct mail. The number of

24   times they've purchased, the value of the purchase.

25   That's the basic information that a single

76

1   magazine would have, that information can become

2   more valuable if you're a multimagazine publisher

3   or you have other lines of publishing so you can

4   then create a broader profile of the person if

5   they're also buying books or magazines in different

6   interests.

7   But the interesting thing about magazines,

8   is that on a -- say a broad interest magazine, one

9   of the seven sisters, when a publisher is trying to

10   promote to the consumer, probably the most useful

11   type of information that the publisher will have is

12   cluster information. If a person is of a certain

13   age and lives in a certain area, that their

14   neighbors may be likely to buy the same magazine.

15   The more specialized you get in a magazine,

16   let's take a woodworking magazine, just because a

17   person lives next door to someone who buys a

18   woodworking magazine, there is absolutely no reason

19   to suppose that the other person would want to buy

20   one.

21   So, the use of the use of data for the

22   small -- the small publisher, the small business,

23   is becoming far more important. We used to have

24   something, until a couple of years ago, called

25   Publishers Clearinghouse and American Family

1   Publishers, which mailed into every household in

2   the country, and the consumer could self select

3   their magazines.

4   Nowadays, those mailings are a thing of the

5   past. And information to a publisher has become

6   far more important, to be able to target their

7   consumers.

8   MS. ALLISON BROWN: Betsy?

9   MS. ELISABETH BROWN: There are fairly

10   significant restrictions on credit card information

11   and data that's used to actually make specific

12   financial offers, from the list compiler companies,

13   like Equifax and Experian. And although I don't

14   represent those companies, I'm not well versed in

15   specifically what those criteria are, the financial

16   services companies that we've worked with, they can

17   only use certain information if they're actually

18   making a credit offer, where they are willing to do

19   a pre-approved credit offer, which means that they

20   are going to say because I have pulled this

21   information on you, I'm willing to say that I will

22   guarantee that if I make this offer, you can have

23   this product.

24   And that data cannot be used by another

25   portion of the bank to make another type of offer,

78

1   whether or not extending credit. So, those

2   protections are in place, I don't have all the

3   details about all the specifics, but it's important

4   to know that they're out there.

5   MS. ALLISON BROWN: Right, and the FTC is

6   very familiar with the Fair Credit Reporting Act

7   and the restrictions on credit data, so that's

8   useful to know, although we are focusing here on

9   data that's not being used for credit decisions.

10   Paula?

11   MS. BRUENING: Yes, I just wanted to go

12   back to the Driver's Privacy Protection Act. I

13   think that that piece of legislation really

14   reflects heightened consumer concern about the

15   incompatible use of this public record information,

16   and it is a response to that.

17   And I think what it does is really offer to

18   individuals who are participating in these basic

19   life experiences, the same kinds of choice that we

20   have come to expect in the commercial realm. We

21   require notice and choice when we're doing business

22   now with a website, or with an organization, and

23   something -- legislation like the Driver's Privacy

24   Protection Act offers that same kind of consumer

25   choice, which I think is critical here.

                    For The Record, Inc.
                     Waldorf, Maryland
                      (301) 870-8025

         1   MS. ALLISON BROWN: Ted?

         2   MR. WHAM: Just a couple of concepts I

         3   would like to throw out there, and I would like to

         4   pierce a couple of notions about what's happening

         5   with data out there.

         6   There is certainly data just being

         7   collected in a permissioned basis. There is also

         8   certainly information which is being collected

         9   which is not personally identifiable and is going

        10   through a more of an aggregation, a blending type

        11   of a process.

        12   Ms. Brown talked about some of the

        13   practices of Claritas, and Claritas uses largely,

        14   if not exclusively, nonpersonally identifiable

        15   information available from census tract records

        16   from U.S. Government surveys through the census

        17   process, but there's an immense amount of data

        18   which is collected which is not permissioned in any

        19   way, so the consumer is not being asked whether it

        20   is okay for that information to be shared with

        21   third parties, and there's an immense amount of

        22   information which is available that is, you know,

        23   personally identifiable and shared with third

        24   parties quite readily.

        25   So, I would have you think, we have an

1   especially erudite audience in terms of knowing how

2   this process works, although we're all here in this

3   workshop, I think a lot of us have an understanding

4   walking in the door how this process works. But if

5   you thought back to your five most recent

6   purchases, I would suspect that there are very few

7   of us in this room who would know whether the

8   companies with whom they did that transaction have

9   a process of sharing that information with third

10   parties, okay?

11   So, you know, think about what you've

12   purchased most recently, and there are many, many

13   companies who the difference between profit and

14   loss for those companies is made by selling their

15   customer information to noncompetitive businesses

16   who are going to be targeting the same type of

17   business.

18   So, if I'm buying a computer peripheral and

19   it's for an obscure, you know, system, other

20   customers that sell computer peripherals to that

21   same obscure system in a noncompetitive way, can

22   almost invariably buy that information.

23   And the best example that I can give of

24   that is the Bible for mailing lists in the United

25   States, the Standard Rates and Data System, SRDS.

1   I have a friend who is a list compiler, and before

2   this session, I called her and I said, How many

3   pages is that book these days? And the current

4   volume exceeds 3,500 pages. Something on the order

5   of 100,000 distinct mailing lists are available for

6   rental in the United States. Most of those, the

7   majority of those, with distinct personally

8   identifiable information in them.

9   MS. ALLISON BROWN: Win?

10   MR. BILLINGSLEY: I would just like to make

11   one other point and discuss an anomaly that we face

12   in our data collection process, in processing

13   warranty information. Some of that data is

14   collected via a web browser technology, fully

15   Internet-based, and clearly when you collect data

16   using that methodology, it comes under the fair

17   information principles of notice, choice, access,

18   security and enforcement, but there is also a large

19   portion of that data that's not collected using

20   browser-based technology. It's collected using a

21   dial-up, a synchronous modem capability with an

22   application that is loaded in the PC.

23   So, some people would make the contention

24   that since you're not on the Internet, that is

25   offline data. Now, you know, we have struggled

82

 1   with how to deal with that issue, and the way we

 2   resolve it in Naviant is we treat data collected by

 3   either one of those two methods by the more

 4   rigorous online marketing data collection rules,

 5   but it is an anomaly that I think should be

 6   addressed so that there is clarity provided in how

 7   people that try to collect data in an ethical and

 8   permissioned way, how they really should operate

 9   when they face these kinds of dilemmas.

10   MS. ALLISON BROWN: I do want to go back to

11   some of the specifics about the data that are being

12   collected here. Betsy, you've talked a little bit

13   about census blocks, zip code information, and zip

14   plus four information. Can you give us a sense of

15   how many households are in a census block, versus a

16   zip code block, versus a zip plus four?

17   MS. ELISABETH BROWN: Yes, a zip plus four

18   would probably be the lowest level of geography,

19   not even geography, because there aren't

20   boundaries, but the lowest level at which you can

21   compile information that's not at household level.

22   And generally a zip plus four can have anywhere

23   from four to ten households in it.

24   Most of the zip plus four data that gets

25   compiled, they have factors in there whereas if

1   there isn't enough information for a particular

2   variable, that is data-filled so that you don't

3   have any privacy issues.

4   The next level up, a block or block group

5   tends to have anywhere from 250 to 350 households.

6   Zip codes can have anywhere from a few thousand to

7   25,000. They're not really cohesive types of

8   geographies. And census tracks are anywhere from

9   1,200 and up.

10   So, low enough levels of geography so that

11   if you're a broad, when you're looking at some of

12   the broad applications that we're talking about,

13   when companies are just trying to understand the

14   lay of the land, for example, generally zip codes,

15   counties, census tracts are a good way for them to

16   really understand what's going on in a marketplace,

17   if they want to enter the marketplace or not.

18   And what we see is that there's different

19   levels of using some of these data. A lot of the

20   clients that we deal with will use a lot of this

21   information for more of their strategic marketing

22   purposes, and when they go out to actually

23   implement a program, they will buy a direct mail

24   list.

25   The attributes that they use to understand

1   their total marketplace may be different than they

2   actually use on the implemented direct mail list.

3   And I think Lynn went over that a little bit, which

4   is that what you'll find is that just because they

5   know that a certain demographic characteristic is

6   currently their, quote, best customer, when they

7   actually go to pull the mailing list, there are

8   many different market -- let's say environments

9   that will cause them to maybe change a specific

10   type of demographic that they're going after, or

11   they'll look at a list and they'll find that the

12   people that they most want to attract, let's say

13   for private banking, are not direct marketing type

14   of customers, that they really aren't going to

15   reach them through a direct marketing list. They

16   don't exist much on the list, there isn't enough

17   data on them and they're not really responsive to

18   the list.

19   So, I think that sometimes people believe

20   that these companies have an enormous amount of

21   information, which they do, but in their practice

22   of actually rolling out marketing programs, it's

23   not as succinct as you might think it is, that they

24   know exactly who their targets are and they can

25   then implement against those targets. They have to

1   really use a lot of strategy and analysis to just

2   try to reach the right person.

3   I don't know if that's a -- there's just a

4   lot of different ways you can use that type of

5   information. So, you can move from these

6   geographic levels down to the household level, but

7   you may not have an exact fit when you do that.

8   MS. ALLISON BROWN: And we heard a little

9   bit in the overview about how businesses append

10   data from third party databases. Can anybody give

11   any specific examples of what types of data

12   businesses append to their in-house customer files?

13   Win?

14   MR. BILLINGSLEY: Well, just having a name

15   and address and a flag that says you're an Internet

16   household is not a very effective product in terms

17   of providing marketing lists.

18   So, that base core of information is used

19   to do a match with various data compilers and

20   aggregators of information, and then we ingest

21   certain attributes that are associated with that

22   name and address. And some of those attributes --

23   and there's many -- but it would be things like

24   income range, age range, gender, hobbies,

25   interests, things of that nature, that we use to

86

1   embellish the marketing file so that we can do

2   selects and generate lists that are targeted for

3   specific products and services.

4   MS. ALLISON BROWN: Does anybody want to

5   add to that?

6   Michael?

7   MR. PASHBY: Generally magazines will

8   append information slightly differently, depending

9   on the type of magazine. A general magazine will

10   probably append more information or have the

11   ability to append more information.

12   I mean, clearly, the very basic information

13   of age, income, family size, gender, is generally

14   available to be appended to the -- to that list,

15   but the more general the magazine, probably the

16   more selections that will be made available.

17   There are a number of companies which will

18   take a magazine list and add information to it,

19   creating that database, and the sort of information

20   that can be appended is everything that's being

21   talked about today. Whether it be the types of

22   cars that people own, when they bought a car, the

23   type of house, the value of the house.

24   There's a lot of information that can be

25   appended, but in general, magazines tend to be the

1   starting -- the starting place rather than the end,

2   with all that information appended to it, because

3   they start -- you're starting with the general

4   interest area, and then it is merged and purged

5   with other lists during the marketing process.

6   MS. ALLISON BROWN: Thanks. Ted?

7   MR. WHAM: A very typical use of appended

8   information is to take a large universe file of all

9   your customers and presume you're a cataloguing

10   business that has, you know, for conversation's

11   sake, a million customers that have done business

12   with you over time.

13   You take a statistically representative

14   sample of that, of perhaps 10,000 individuals and

15   you go and append absolutely everything to those

16   10,000 people you can possibly get our your hands

17   on, from income, age, whether they've got children,

18   the age of those children, whether they're

19   grandparents, the type of interests that they have,

20   all of the psychographic information, everything

21   you can get to that.

22   And then you run that against statistical

23   processes and say, Okay, tell me of all of these

24   different processes, which one of these are going

25   to be predictive of the ones I care about most.

1   And as Ms. Wunderman pointed out this

2   morning, different businesses care about different

3   things. Some businesses want lots of transactions,

4   some businesses need to be very concerned about

5   turnover, loss of the customers, some long distance

6   carriers and cellular phone carriers, for instance,

7   are extremely interested to make certain that

8   they're getting customers who are going to stick

9   with them and are not switchers and so forth. And

10   it varies by businesses.

11   Once they identify which of those

12   characteristics are particularly predictive for the

13   customers that they want, they will then go to the

14   remaining universe, those 990,000 names that they

15   never did anything with, and they'll go back to the

16   original appending firm and say, Please append

17   these two or three variables that I want. Much

18   more cost effective than appending all 30 or 50 or

19   150 variables to the entire universe if only three

20   of those are going to be productive for what you're

21   trying to do.

22   MS. ALLISON BROWN: Betsy?

23   MS. ELISABETH BROWN: Yeah, that's a very

24   good point. I think one of the reasons that

25   Claritas has been in business for 30 years is that

1   one of the things that we have been able to do is

2   boil down a lot of those characteristics into

3   segment codes, which makes it a lot easier.

4   I mean, we have seen in the financial

5   services arena about ten years ago, they were one

6   of the first industries to really take customer

7   file records that they have done, they have a very

8   -- financial institutions tend to have a very

9   strong relationship, we talked about what a

10   relationship was, with their clients. There's a

11   lot of trust there that the clients are giving a

12   lot of very in-depth financial information to these

13   companies.

14   Financial services companies are fairly

15   conservative from what we've seen with what they do

16   with the collected information, but in addition,

17   they didn't really have the databases and the

18   software capability to manipulate these gigantic

19   files with so much information that they collect,

20   nor did they have a good way of updating them.

21   So, even with them collecting all of this

22   very personal information, they tended to use

23   companies like Claritas to help them boil it down

24   and understand from a one code type of an aspect

25   what can we know about these people quickly and

1   easily without having to look at 100 or 200

2   different variables that we've collected over time.

3   So, that's sort of in essence what a

4   cluster code is. The basic information we really

5   need there is just an address that will allow you

6   to say the likelihood is that these people live in

7   an upscale suburban neighborhood or an upscale

8   urban neighborhood. And a real quick example of

9   how that would be used would be if you knew -- if

10   you just had straight demographics on someone and

11   you knew you had two males, 30 years old, and you

12   figured out that they make about $50,000, do they

13   need individual life insurance or not.

14   Not quite enough information for you to

15   make a decision on that, one male might be single,

16   doesn't own a home, doesn't really have any

17   dependents, where the other male might have a

18   family with three kids, a house, a mortgage, so

19   having a little bit more rich information on that

20   would make you look at these two similar

21   demographics and say I'm going to offer insurance

22   to the one because they are going to need it and

23   not the other.

24   Or another quick use is if they're only

25   using their internal data and they know that they

1   have got a thousand people who have $5,000 in their

2   checking account and always have had $5,000 in

3   their checking account, by overlaying some of these

4   segment codes, you can get a quick idea that five

5   of those people, that's all they're really ever

6   going to have in demand deposits at a bank, that's

7   really all they're qualified to have, and this

8   segment code would be something like a number, 27,

9   that would represent a string of demographics that

10   would predict that that person is probably in that

11   demographic.

12   And you might find out that half of these

13   people have a very high likelihood for using a loan

14   product. So, if you wanted to offer them another

15   service, you would be better off offering them a

16   loan product than the other half who you would be

17   better off offering an investment product.

18   So, without having to know a ton of

19   personal information, you can at least make some

20   good guesses as to what the next most likely

21   product is to offer those people.

22   MS. ALLISON BROWN: And can you give us a

23   couple of more examples of the segments, I think

24   that Mary in the overview gave us a couple from a

25   newspaper article, I think people might be

92

1   interested to hear what some of the other ones are

2   and how many there are as well.

3   MS. ELISABETH BROWN: Well, we have --

4   there are several different segmentation systems,

5   and a segmentation system really starts off as just

6   a predictive model. So, as Ms. Wunderman was

7   saying earlier in the session, different industries

8   care about different data.

9   So, a very generic model would be something

10   like our Prism segmentation system that's based on

11   the demographics of where you've settled, where you

12   live, there are several more like that out there in

13   the public domain, and they have -- some of them

14   have nicknames, they tend to be sort of upscale

15   suburban, like Blueblood Estates, Urban Singles,

16   Upscale Urban Singles, Midscale, you know, Urban

17   Dense Areas.

18   So, there's lots of different ways that you

19   can just get a quick snapshot of what the

20   settlement patterns are in that neighborhood.

21   And one of the things that we've -- because

22   these things, as everyone said, as I think Paula

23   was saying earlier, there's different uses for

24   that. It's important to know that you're in a

25   suburban market area if you're trying to sell lawn

93

 1   mowers.   You certainly don't want to be offering

 2   that to urban upscale singles in high rises.

 3   So, some of the data is critically

 4   important to some of the things you're trying to

 5   sell.   It may not be very important at all to

 6   somebody who is selling a very targeted niche

 7   magazine that could appeal to many different people

 8   and has no relationship in terms of a geographic

 9   reference.

10   So, there are 62 Prism clusters, which

11   means that we have predicted 62 different

12   neighborhood settlement patterns.

13   Another segmentation system is based more

14   on predicting financial services behavior, or

15   telecommunications behavior. In those segments,

16   there are about 42 of the financial patterns, and

17   they are anything from upscale suburban families

18   with children, upscale suburban singles, upscale

19   urbanites, those type of cluster types or segment

20   types, and that's more based on a specific range of

21   income, asset prediction, age and presence of

22   children.

23   So, those -- they're slightly different,

24   but, you know, basically you can start with

25   anything. In our audit of the convergence data,

1   which is the telecommunications, I think we have

2   about 57 different segments and they're based on

3   patterns of usage that we have seen in terms of

4   product usage, and then on the back end, we infer

5   the demographic segment for that.

6   MS. ALLISON BROWN: Ted?

7   MR. WHAM: There's a distinction which

8   might be valuable for the FTC in doing this,

9   there's two major categories of lists that you can

10   consider. One would be compiled list information,

11   the other being response list information.

12   Compiled list information tends to be very

13   broad coverage, it's information about who you are,

14   whereas response list is more information about

15   what you've done, what type of products you've

16   done.

17   So, if I want to buy something that has a

18   very broad geographic coverage because I'm offering

19   a service that has something which is primarily

20   defined upon where people live and the types of

21   birds of a feather flock together type of analogy

22   that is the basis for Claritas' business, then I am

23   going to want that type of a compiled list.

24   If I'm trying to find people who have

25   interest in doing very specific types of activities

1   and so forth, I am going to want to buy lists from

2   similar businesses or businesses that point to

3   similar types of people.

4   Response lists tend to be very narrow. I

5   can't typically take a response list and very

6   effectively use that as an overlay tool against my

7   universe of customers, and say tell me additional

8   things about this, because if I took my, you know,

9   300,000 customers and matched them against somebody

10   else's 300,000 customers, I might find, you know,

11   700 that match between those two of them.

12   I would have a rich data set for those, but

13   I wouldn't have enough to make it economically

14   worthwhile to do that.

15   Right now it's very easy to go from the hub

16   out to the spokes. Go to a company that sells a

17   specific product and tell me all of the customers

18   for that product or set of products that they sell.

19   It's extremely difficult to say that I want

20   to start at a spoke and tell me all of the hubs

21   that they're attached to, so go to a specific

22   customer and tell me all of the products that they

23   have bought within a category, or perhaps even all

24   the products they have bought.

25   I will say that although you can't do that

1   today, there's an enormous economic potential

2   there, and I am certain that many, many very bright

3   people have spent a lot of time trying to figure

4   out how I can come up with a master universe of all

5   of the computing products that somebody has bought,

6   or all of the clothing purchases that somebody has

7   bought, because if I can do that, and if I'm a

8   marketer selling, you know, an upgrade to a

9   particular type of computer, that's the golden

10   list, and I will spend a lot of money to rent names

11   from that list.

12   MS. ALLISON BROWN: Michael?

13   MR. PASHBY: Yeah. I think in the magazine

14   industry, one of the most important sets of data

15   that can be added to a magazine list is catalog

16   information, and the merging of catalog

17   information, because it does add the recency,

18   frequency and value component to the magazine list.

19   If you go back to the woodworking magazine,

20   a person may buy a woodworking magazine noting that

21   they're interested, but if you can match that with

22   catalog information about the purchase of tools or

23   the purchase of other supplies, and they're showing

24   some frequency there, that separates out one group

25   of people who are peripherally involved to

1   high-volume purchases within that area, and I

2   suppose it also gives a greater degree of value to

3   the broader lists, like a news magazine or a seven

4   sisters magazine, those people may be then

5   segmented into very specific interest areas.

6   So, you have a -- one of the seven sisters,

7   but you can match that with kitchen and food

8   catalogs to show a high interest in cooking. So,

9   it then becomes much more interesting for other

10   marketers, and much more targeted to the consumer.

11   MS. ALLISON BROWN: And what do businesses

12   do to ensure that the data that you collect are as

13   accurate as possible?

14   Win?

15   MR. BILLINGSLEY: Well, we do several

16   things. Marketing data does not have to be 100

17   percent accurate to be effective, but you want to

18   make it as accurate as you possibly can, within the

19   economic constraints that you have to deal with.

20   But an example of some of the things that

21   we do to make sure our data are accurate, even if

22   you permissioned us to use your data in a product

23   registration effort, you say yes, I would like to

24   receive offers from third party -- from third party

25   marketers regarding products and services that

98

1   would be of interest to me.

2   You don't automatically go into Naviant's

3   database just because you have permissioned us. To

4   make sure that we're doing that accurately, we

5   match your name and address against a public data

6   source to make sure that you really are who you say

7   you are. That helps us get out the Donald Ducks

8   and the Roy Rogers and some people who like to play

9   games, but we find the utilization of the public

10   compiled data, a very meaningful tool to ensure

11   that our file is as accurate as it possibly can be.

12   MS. ALLISON BROWN: And can you just

13   clarify what you mean when you say public sources

14   of data and compiled sources of data? Can you be

15   more specific?

16   MR. BILLINGSLEY: Well, I probably

17   misspoke, I probably should have said compiled

18   sources of data which originated from public

19   sources of data. But it's a very effective way to

20   make sure that data is accurate.

21   The other advantage that it holds for us is

22   that we're very sensitive in not collecting data on

23   children, and so by matching the name and a

24   registration with an aggregator's data or a

25   compiler's data, kids don't buy real estate

99

1   property and cars and things of that nature.

2   MR. WHAM: You haven't met my brother.

3   MR. BILLINGSLEY: So, it gives us a

4   reasonable check to make sure that we're not

5   collecting data on children.

6   The other thing that we do to make sure

7   data is accurate is we use the DMA suppression

8   file, and we find that a very effective way to make

9   sure that we don't include data in marketing lists

10   to the people who have gone to the trouble to go to

11   DMA and sign up for either their direct mail

12   suppression file or telemarketing suppression file,

13   and a new product they started just a few months

14   ago which is an email suppression file.

15   So, that's another way to make sure that

16   the data we provide a marketer is accurate. And

17   the third way is the good old U.S. Post Office.

18   All marketers use the NCOA process, or should use

19   the NCOA process.

20   MS. ALLISON BROWN: And what does NCOA

21   stand for?

22   MR. BILLINGSLEY: National Change of

23   Address. And the way that basically works is if

24   you move and you fill out a card at the Post Office

25   so your mail will be forwarded to your new

1   location, that information is collected by the Post

2   Office, and the Post Office has this very large

3   file of people who have relocated that's utilized

4   to redirect their mail. And the Post Office

5   authorizes some 20-something companies to take this

6   data and do a match to make sure that if you have

7   an old address in your file, and you match the old

8   address, then you can substitute the new address.

9   And that's something that's been in

10   existence for a long time, it's been used in the

11   direct marketing world for a number of years. It's

12   a very effective tool to make sure that if you're

13   doing a direct mailing of a marketing list, that

14   the marketing collateral that you're spending hard

15   dollars for to be delivered by the Post Office is

16   truly deliverable.

17   MS. ALLISON BROWN: Thanks.

18   Michael?

19   MR. PASHBY: Some information really has to

20   be accurate. Some years ago I marketed a magazine,

21   which I won't name, but, well, let's say a parents'

22   magazine, and our primary source of readers were

23   parents of newborn children.

24   We were extremely sensitive to the problems

25   inherent in that. Somebody's buying lists of

1   potential new births, and some births obviously are

2   not live births, and you are mailing to people

3   saying congratulations, and that can be extremely

4   sensitive, obviously.

5   So, correcting data is very, very

6   important. We spent an awful lot of time and

7   energy making sure that the sources we were

8   compiling that data from were accurate. If we

9   found that there was an incidence of inaccuracy, we

10   would cut off from that source. And we would not

11   buy information from that source ever again.

12   Because of the responsibility to the consumers that

13   we had.

14   MS. ALLISON BROWN: And can you be a little

15   more specific about what the sources of that type

16   of data are?

17   MR. PASHBY: The sources of that data were

18   from -- no, I can't, they were from compilers. It

19   would come from doctors' office visits, from

20   insurance companies, from a lot of different

21   sources, I believe.

22   MS. ALLISON BROWN: And what did you do to

23   make sure it was accurate? How did you gauge that?

24   MR. PASHBY: We would -- we would do it

25   from the complaint level. That was the difficulty.

102

1   You were doing it after the event, but if one found

2   that there was a degree of inaccuracy there, then

3   we would cut off from that source.

4   MS. ALLISON BROWN: Ted?

5   MR. WHAM: You talk about data quality

6   issues, it's useful to look at it in two different

7   ways. There's the quality of the data at the time

8   that it's collected, and there can be errors

9   introduced through typographical errors, or to

10   purposeful, you know, fraudulence, Mickey Mouse and

11   so forth, but there's also a more significant issue

12   of data decay.

13   Like if I, you know, show up in a database

14   that I'm 25 to 34 years old, how old am I tomorrow?

15   Okay? So, date range information is very

16   inaccurate. Births, deaths, marital status and so

17   forth, and people moving all the time, but we have

18   a very mobile society. So, the statistic that I

19   heard, I can't vouch, say, for this, but the

20   average data in a data base decayed at a rate of

21   about one and a half percent per month, that was

22   the inaccuracy that built up over time.

23   The marketer has an absolute vested

24   economic interest in making sure that that

25   information is as accurate as possible. If it's

1   inaccurate, they can't use it for the goal that

2   they have. So the alignment of the market

3   interest, the consumer's interest of having

4   accurate information is absolutely, I mean,

5   perfectly together.

6   MS. ALLISON BROWN: We have time for one

7   more comment and then we will go to questions from

8   the audience.

9   Betsy?

10   MS. ELISABETH BROWN: One of the things

11   that I wanted to talk about data accuracy is that

12   from the Claritas standpoint, we've seen a lot of

13   different types of data. We not only use Census

14   data and other public domain data, consumer

15   surveys, which is really self-reported demographic

16   information, but in order to -- as I was talking

17   about implementing, in order to actually implement

18   an actual marketing program, we will take our

19   segmentation codes and place them on list files,

20   such as Acxiom, InfoUSA, Experian and Equifax, and

21   many other compiled lists.

22   What we have found many times, especially

23   when we're using the types of models that I

24   discussed earlier that go down to a more specific

25   household level, in terms of the demographic

104

1   variables that we say are predictive of the

2   behavior that we're trying to help our customers

3   use, what we find sometimes is that these list

4   sources have, I guess, decay, some other

5   information, missing information, fill-in models,

6   and we will show them that the data that we have

7   proves out that their list is not really

8   distributing the way the U.S. population

9   distributes down to a low level of geography, a zip

10   code, a census tract, a block group.

11   So that we can take a look at a list of

12   data out there and say you're reporting that only

13   two percent are in the income category, 50,000

14   plus, and we expect to see more like 27 percent.

15   So, we have actually created models that

16   help some of these list sources to improve their

17   models, their income models or whatever that might

18   be, to base them more on sort of a benchmark of

19   data.

20   So, there's a lot of -- it's sort of a

21   symbiotic relationship, back and forth with

22   Claritas and the list providers, sometimes they

23   actually do change some of their model information

24   on their file based on our information, and other

25   times we just use it to assign what we think is a

1   more appropriate segment code, then they don't

2   necessarily change that source of data, it depends

3   on how they prioritize their models, and they

4   prioritize their input sources.

5   MS. ALLISON BROWN: And I believe that

6   Claritas also updates Census data, how do you do

7   that?

8   MS. ELISABETH BROWN: On an annual basis.

9   We update census data, again, from a list of a lot

10   of sources, some of the postal information, some of

11   the moving information, NCOA. There's a lot of

12   intercensal data that is produced that's not

13   produced on 100 percent factor.

14   In other words, there are many, many

15   counties, communities and states that do many

16   updates of data and information, and we take really

17   whatever we can get that's available and utilize

18   that data. There are also many models that we have

19   perfected over time, and we've been doing this,

20   this is our third census that we've been actually

21   updating information where we just do projections

22   and straight line information based on other data.

23   So, there are many sources that we can use,

24   both census-type sources that we think we can have

25   a high degree, feel that we have a high degree of

1   accuracy in terms -- and relevance, and some of the

2   consumer survey research that's out there just

3   allows you to take a look at shifting data in terms

4   of how people are self reporting where their

5   incomes are.

6   And in addition, we do use a lot of the

7   list data just to try to get a handle on which

8   areas are growing. Postal drop rates, I think ADVO

9   counts, which is another list source where they

10   constantly are updating where the postal drops are

11   going.

12   MS. ALLISON BROWN: One thing that becomes

13   clear pretty quickly is how integrated the

14   aggregators are with the sources and how the data

15   sort of rotate in and out of the different

16   databases.

17   I know when I open up the discussion for

18   questions from the audience, if you have a question

19   you would like to ask, please raise your hand and I

20   will recognize you after one of our staffers comes

21   over with the wireless microphone. Please speak

22   into the microphone while asking your question and

23   state your name and organization before you begin

24   your question so the court reporters can get an

25   accurate transcript of today's proceedings.

1   MR. CATLETT: Thank you, I'm Jason Catlett

2   from Junkbusters. I have a question for Mr.

3   Billingsley. I have an advertisement in a trade

4   magazine from Naviant, it's quite amusing, it shows

5   a biker with tattoos and a beard, and it makes

6   light of the fact that he likes roses, and when

7   you're going online, you might want to -- I infer

8   from this advertisement -- you might want to pitch

9   a banner advertisement for roses.

10   Could you please tell us the process by

11   which when this biker goes online and visits a

12   website the website would know that he likes roses?

13   MR. BILLINGSLEY: Well, I'll talk a little

14   bit more about that this afternoon, if you would

15   like, because we'll talk about how the data is used

16   to administer marketing programs, but basically, we

17   would have business relationships with some of the

18   ad serving companies that collect data anonymously.

19   We would pass data attributes to those ad

20   serving companies anonymously, so that they could

21   then target a banner ad that was appropriate for

22   that particular person, without ever knowing the

23   person's name.

24   MR. CATLETT: Thank you.

25   MS. ALLISON BROWN: Don't forget to say

 1   your name and affiliation for the record.

 2   MR. HENDRICKS: Thank you, Evan Hendricks,

 3   Privacy Times. I had one question, but first I

 4   wanted to follow up on what you said about the

 5   babies, because we always wondered about that, a

 6   lot of us.

 7   So, is it the doctor's offices would sell

 8   that information, or the insurance companies were

 9   some of the sources for people who are about to

10   have babies?

11   MR. PASHBY: I am not absolutely certain, I

12   believe that was, and this was some time ago.

13   MR. HENDRICKS: But I also wanted to

14   comment, hospitals and birthing classes, and do

15   they sell it to a compiler, is that how it would

16   work?

17   MR. PASHBY: It's my belief that that's how

18   the information was compiled.

19   MR. HENDRICKS: Okay. The other thing is

20   you said that the magazines, I think correctly, are

21   at the front end of this process, much more so than

22   some of the others who are at the back end, and in

23   the UK, on a subscription form, the little cards

24   that you get in your magazine, you have a check-off

25   box, it says if you don't want your name shared,

1   check here, and send it in with your subscription,

2   and one of the big problems in the U.S. is that at

3   the point of the collection of data from

4   individuals, people are not notified what could

5   happen or given the chance to even opt out.

6   And so, do you think that makes sense from

7   a data practices point of view, and do you think

8   that your association is ready to sort of endorse

9   that and recommend it, you know, considering the

10   growing strong feelings about privacy?

11   MR. PASHBY: I think from the standpoint of

12   having to fill in, check a box on a card, what we

13   found in any promotional activity, having the

14   consumer take actions in a promotional activity

15   reduces the response. Therefore, we have cards

16   which are prechecked, and yes I want this magazine,

17   and then all they have to do is tear the card out

18   and put it in the mail.

19   But as I mentioned, we also do publish in

20   the magazine the privacy policies and the ability

21   to -- and the ability to call an 800 number or send

22   to the magazine fulfillment house to be taken off

23   the list.

24   MR. HENDRICKS: And of course what I'm

25   describing wouldn't even, I mean someone could

 1   still take the card and just throw it in the mail.

 2   It's only those people that took the time to look

 3   and see that there was a check-off box, and could

 4   check off they didn't want their name sold.

 5   So, what I'm saying is would it interfere

 6   with, you know, with what you're saying? I mean,

 7   it wouldn't require the individual to check the box

 8   to say I don't want my name sold, it would only be

 9   for those individuals that cared enough. And if

10   this is practice -- am I confusing you? You look

11   like you're not following me.

12   MR. PASHBY: I'm saying that any time there

13   is -- you give people the option in a promotion,

14   the response declines. And as we mentioned before,

15   the whole use of information has been more

16   effective and more efficient when we are spending

17   or when businesses are spending 65 cents to a

18   dollar to put a piece of promotion into the mail

19   and you're getting single digit responses, you're

20   trying to be as efficient as possible.

21   MS. ALLISON BROWN: Ted, do you want to

22   comment on that?

23   MR. WHAM: Yeah, I absolutely would. The

24   basic fundamental question is if I -- if consumer X

25   chooses to do business with Business Y, should

1   consumer X have the opportunity to say Business Y,

2   don't contact me. That's question A.

3   And question B is, Business Y, don't

4   share my information with company Z and Z sub

5   one and Z sub two and so forth. I fundamentally

6   reject the notion that a consumer should be able

7   to say I want to do business with a particular

8   company Y, but that company can't follow on and

9   make money out of that relationship. I think

10   that that has terribly negative consequences

11   for the efficiency of economic transactions in

12   this country.

13   The reason we don't have mom and pop stores

14   in the United States very successfully anymore and

15   the reason we have Wal-Marts in this country is

16   because they provided a very economically efficient

17   way of delivering low-priced goods in the United

18   States, for better or for worse, but the wheels of

19   that continue to turn by having the businesses be

20   able to use that information in the most effective

21   way possible.

22   MS. ALLISON BROWN: We are trying to stay

23   on a factual level here and stay away from policy

24   discussions.

25   MR. WHAM: I couldn't help myself.

112

1   MS. ALLISON BROWN: Does anybody else have

2   a question?

3   MR. DIXON: Tim Dixon from Baker McKenzie.

4   A question, just to pick up on that point to take

5   it a little bit further. When we talked,

6   particularly when you mentioned the 30 million

7   permissioned people or households in the database

8   that you've got, what proportion do you know is

9   that people who have done the sort of check box as

10   opposed to the kind of I guess you could call it

11   permission by inertia where they would need to read

12   a privacy policy and then go through an active

13   process of say opting out if they wished to opt

14   out?

15   MR. BILLINGSLEY: I don't know the

16   percentage. We use in collecting the data, and

17   this is primarily a decision that's made between us

18   and the client that we're providing registration

19   services for, we use three different kinds of

20   permissioning processes. I'll try to get through

21   this without confusing myself and the audience, but

22   we use the opt-in process, which we define as a

23   permissioning question with either yes or no, not

24   preselected.

25   We also use the opt-out permissioning

1   process, which is a permission question with

2   yes preselected, and in certain situations,

3   not a lot, we use the explicit process, which

4   basically is a bold statement that says, Do

5   not provide us your marketing information unless

6   you're willing to receive, you know, marketing

7   offers.

8   So, we utilize all three of those,

9   depending upon the circumstance. We do flag how

10   the permissioning process worked for that

11   particular consumer, and we are sensitive based

12   on the permissioning process, how that

13   information is used when it is -- when a

14   marketing program is generated based on that

15   permissioning.

16   But the percentage, I don't know the number

17   to be very specific about your question.

18   MS. WOODWARD: My name is Gwendolyn Woodard

19   with Worldwide Educational Consultants. I'm

20   consumer A, and I decide that I'm going to attend a

21   conference, so I go online and complete the form.

22   The site that I'm going to complete the form on has

23   a third party advertising network associated with

24   it, okay? As I complete the form, I notice in the

25   URL the information that I put in the form is

114

1   reflected up there.

2   So, as a consumer, how would I know how

3   that information is going to be used, what

4   databases will it be going to, especially if this

5   third party advertising network uses a push and

6   pull technology to disseminate that information to

7   different databases?

8   MS. ALLISON BROWN: Does anybody want to

9   take that on?

10   MR. WHAM: It's very useful if you're

11   omniscient.

12   MR. BILLINGSLEY: I'll respond a little

13   more. The --

14   MR. WHAM: Comprehensively, perhaps.

15   MR. BILLINGSLEY: Yeah. The way it should

16   work, in my opinion, is if you're in that kind of

17   situation where a redirect is occurring, without

18   your knowledge, then the privacy policy should be

19   very explicit in saying -- in discussing the

20   redirect to another website, why that is occurring,

21   what your choices are to either participate in that

22   or not participate in that. And disclosure, in my

23   opinion, is the key for the consumer in

24   understanding what is or is not happening to

25   their data, particularly when you see it in the

115

1   URL.

2   MS. ALLISON BROWN: And let me just say

3   that that's really a question that should be

4   directed to network advertisers, and none of the

5   panelists up here represent any network

6   advertisers, and it's really a separate issue that

7   we're not addressing today. But, you know, that's

8   a question for other people.

9   We are running out of time. Paula, did you

10   want to comment on that issue?

11   MS. BRUENING: No, thanks.

12   MS. ALLISON BROWN: So, I think we are

13   going to break for lunch now, and we would like to

14   see everybody back at 1:00, and I want to thank the

15   panelists for a very informative discussion.   We

16   really learned a lot.

17   (Applause.)

18   (Whereupon, at 11:30 a.m., a lunch recess

19   was taken.)

20

21

22

23

24

25

116

```
 1                       AFTERNOON SESSION

 2                 -    -    -    -    -    -

 3

 4     SESSION 3:   WHAT ARE THE BUSINESS PURPOSES FOR

 5     MERGING AND EXCHANGING CONSUMER DATA?

 6

 7     MARTHA LANDESBERG, Attorney, FTC, Moderator

 8

 9     PANELISTS:

10

11     MARTY ABRAMS, Executive Director, Center for

12     Information Policy Leadership

13     JOHNNY ANDERSON, Chief Executive Officer, Hot Data,

14     Inc.

15     C. WIN BILLINGSLEY, Chief Privacy Officer, Naviant,

16     Inc.

17     JERRY CERASALE, Senior Vice President, Government

18     Affairs, Direct Marketing Association

19     PETER CORRAO, Chief Executive Officer, Cogit

20     Corporation

21     LYNN WUNDERMAN, President/Chief Executive Officer,

22     I-Behavior, Inc.

23

24

25
```

```
 1                    SESSION THREE

 2       WHAT ARE THE BUSINESS PURPOSES FOR MERGING

 3              AND EXCHANGING CONSUMER DATA

 4             -    -    -    -    -    -

 5             MS. LANDESBERG:  If everyone would please

 6    take a seat, we would like to get started.  We have

 7    a very full afternoon.

 8             Good afternoon.  My name is Martha

 9    Landesberg.  I'm an attorney in the Division of

10    Financial Practices here at the Federal Trade

11    Commission.  Let me just state, before we get

12    going, we have a couple of announcements to make.

13    I want to reiterate for everyone our ground rules.

14             We request that you turn off your cell

15    phones, please.  Once again we are going to very

16    gently but firmly hold our speakers to the time

17    limits we've discussed with them.  My colleague,

18    Allison Brown, will be your timer.  She's right

19    here, so just look for a sign from her that you're

20    coming toward the end of your time, if you would.

21             We will as time permits again have a

22    question and answer session.  I'll ask again that

23    you please identify yourself for the court

24    reporters before asking your question.

25             And finally, the record of the workshop
```

 1   will be open until April 13 for submission of any

 2   comments or materials you want the Commission to

 3   consider, and we invite you to participate in that

 4   process.

 5   And also a fond welcome for those of you

 6   listening on the audiocast. We apologize and

 7   understand there was some trouble this morning. We

 8   hope things are up and running, and we're happy to

 9   have you with us.

10   One last comment, Michael Pashby in our

11   prior panel has submitted a written statement

12   regarding his comments on the use of medical

13   records to identify new prospects, and that

14   statement, as others, will be posted in the

15   workshop record for everyone to have a look at and

16   comment upon.

17   Now, it's my pleasure to begin session 3 of

18   our workshop, and this is where we really get to

19   the meat and potatoes of what it is that businesses

20   do with all the information we've been hearing

21   about all morning, and what we're going to do here

22   is have presentations from each of our panelists

23   one by one. I'll introduce them one at a time, and

24   we'll take it from there, and as time permits have

25   some questions too.

1   We'll begin with Marty Abrams. Marty is

2   the Executive Director of the Center for

3   Information Policy and leadership at Hunton &

4   Williams. Before joining Hunton & Williams Mr.

5   Abrams, or Marty, spent 12 years as Experian

6   leading their information policy and privacy

7   efforts.

8   Marty?

9   MR. ABRAMS: Thank you very much. As we go

10 through this technical process of keying up my

11 presentation, I would first like to thank the FTC

12 staff for inviting me here this afternoon, and I

13 would also like to thank them for the excellent

14 program this morning. I found it incredibly

15 worthwhile and very informative, and hopefully we,

16 this afternoon, can be just as informative.

17   And we are talking about the uses and

18 purposes for third-party data, and I think that the

19 best place to start with understanding third-party

20 data is understanding that it matches with in-house

21 data, and it begins with the in-house data because

22 that's what marketers begin with, their own

23 customer base, understanding their own customer

24 base.

25   And that data comes from multiple sources.

 1   The most important of those sources is directly

 2   from their customer, and the second is their

 3   relationship with their customer, and this is the

 4   majority of the data that the organizations,

 5   marketers, have in their databases and their files.

 6   And to understand that data, to make the

 7   best use of that data, they have to match that up

 8   with third-party data, and I'm going to be talking

 9   about purposes and not processes. I have

10   colleagues on this panel who I think are going to

11   get more into the processes, but I would like to

12   really put the emphasis on why the data is used.

13   And there's a paper that really goes in to

14   how this works that was released yesterday by the

15   Privacy Leadership Initiative and ISEC Council of

16   the DMA, and that paper is available on the DMA web

17   site I believe.

18   The first process, the first purpose, the

19   first reason for using third-party data is just to

20   make sure that your file is clean. 20 percent of

21   the American population moves each year. People

22   use variations of their names. They use variations

23   of spellings of their name. I'm Marty Abrams. I'm

24   Martin Abrams. I'm Martin E. Abrams. I've lived

25   in California. I've lived in Ohio. I've lived in

121

 1   Texas.   I sometimes buy from my office.

 2   So one of the purposes is to merge all of

 3   those Marty Abrams that are sitting on a company's

 4   file into one Marty Abrams so that I can market

 5   that to me in a unified fashion.

 6   The second is to have a deliverable

 7   address.   We often have multiple addresses,

 8   multiple variations of our addresses.   We

 9   abbreviate our address.   We move, and one of the

10   purposes of using third-party data is to put that

11   data together to have an address that is

12   deliverable.

13   And having a deliverable address means that

14   you can deliver up to 15 percent more of the mail

15   that you mail on a regular basis, and that has

16   really cost implications for an organization.

17   The second purpose is to truly understand

18   your own customers, and I think Lynn Wunderman did

19   a great job of describing that this morning.

20   You're trying to understand what is similar about

21   your customers and what is different, and one of

22   the ways you do that is overlay your file with

23   demographic information from a third-party.

24   Examples of the type of data that you might

25   overlay is age because age is very predictive of

122

1   where you are in your life-style, what you might

2   buy and also inferred or modeled income, and again

3   we have no exact income on any files other than the

4   IRS's files, and those, of course, are not

5   available, so we model income to be able to try to

6   figure out how individuals are similar or

7   different.

8   And that information helps us understand

9   who to market to, how to market to them, what type

10   of products we should offer them in the future. We

11   begin to understand what is predictive of who's a

12   buyer and what is just really a red herring, not

13   very predictive.

14   And then based on what we understand about

15   our own customers, we can go out in to the

16   marketplace and find individuals who are very

17   similar to our own customers, folks who have very

18   similar demographics, very similar psychographics,

19   so we can begin to build our customer base with new

20   customers who are similar to the folks that we are

21   marketing to at the moment.

22   And those sources include competitors,

23   because organizations do exchange lists,

24   noncompetitive marketers, and lastly aggregators or

25   compilers, organizations that put together files of

123

1   individuals for other organizations to use who

2   create mailing lists, and the results are more

3   effective communication with existing customers.

4   We can put together the right message for

5   the right consumer at the right time to maximize

6   that relationship with the customer.

7   We also find prospects who we have the

8   greatest probability of reaching, folks who are

9   most similar to our existing customers, and more

10   important, in this modern age, is we begin to

11   understand how our customers are changing so we can

12   begin to develop the products and services that are

13   responsive to where our customers are going over

14   time.

15   Martha asked me to talk a little about the

16   differences between marketers and aggregators in

17   terms of the type of data they have and the type of

18   processes. When you think about marketers, the

19   folks who actually market to you and I, first their

20   data primarily comes from their own customers.

21   Even if I overlay with data from third

22   parties, if I'm a marketer, most of the data I have

23   is from my own customers. Most of that data is

24   either self reported, I give you my name and

25   address, I volunteer information with you, or comes

124

1   from my own experiences with you as a customer.

2   And lastly, I as a marketer typically have

3   regular contact with my customer and can

4   communicate with you as my customer about both what

5   I'm selling and my processes and the choices that

6   you have.

7   Aggregators have data on a broader

8   population. Some aggregators have most of the U.S.

9   population. The data comes from many, many

10   sources. As we discussed, some of them are public

11   record sources. Some of them are surveys. Some of

12   them are purchase data, but the data comes from

13   many sources, not a single source.

14   Typically the data that is held by an

15   aggregator is not experiential data. It tends to

16   be demographic or psychographic data, and, last,

17   typically the aggregator does not have regular

18   contact with the customer, the consumer, but rather

19   relies on the party that collected the data to have

20   had that contact with the consumer, and most

21   aggregators build systems to make sure they only

22   get data from reliable sources.

23   Thank you very much.

24   (Applause.)

25   MS. LANDESBERG: Thank you, Marty.

125

1   Next we'll hear from Win Billingsley, the

2   Chief Privacy Officer of Naviant. Win?

3   MR. BILLINGSLEY: As we talked this

4   morning, Naviant's key value that they bring to the

5   marketplace is that we provide a database of

6   consumers that are Internet enabled, and we sort of

7   phrase our mission statement as Naviant is a

8   leading provider of integrated, precision marketing

9   tools for online and offline environments, so we

10   can send marketing messages or marketing campaigns

11   to consumers either through direct mail or through

12   Email or through banner ads, so we work in both of

13   those worlds and actually try to integrate those

14   two worlds together.

15   So we enable marketers to reach and build

16   relationships with online consumers, and that's

17   really Naviant's key sole business purpose.

18   It's always tough to get a business model

19   on one slide, so I tried to simplify this as much

20   as I possibly can but still make it meaningful for

21   you, and for Naviant the world begins with

22   electronic registrations.

23   We work with manufacturers that build

24   computer hardware, computer software, and we

25   facilitate the registering of their products and

126

 1   services via the Internet. Most of that data, once

 2   it's captured, is passed back to the original

 3   manufacturer. We keep the name and address and

 4   designate a flag that this individual, since they

 5   registered their product or service via the

 6   Internet, is an Internet enabled household.

 7   So the data point for us begins with the

 8   name and address and an Internet household. That

 9   begins the database processing, and there's data

10   hygiene work that's applied to that database. I

11   talked about it a little bit this morning. We use

12   the compiler's information to make sure the names

13   that we have are accurate in our database.

14   We also append to that from the compilers

15   various data attributes that enrich the data and

16   make it meaningful and store and maintain the data.

17   We also use the DMA's file suppression list to make

18   sure that no one is in our database that has

19   expressed an interest not to be.

20   And I should have mentioned back in the

21   registration process that there is a permissioning

22   process that we go through before you ever really

23   enter into this diagram.

24   So once the data is there with an

25   enrichment of data attributes, then we have the

127

1   ability to deliver this data for marketing purposes

2   in a variety of channels in a variety of ways, so

3   the data can be used to administer direct mail or

4   Email campaigns. It be used to deliver direct mail

5   campaigns, telemarketing and targeted banner ads.

6   And we analyze the data to determine counts

7   based on criteria. A client will come to Naviant

8   and say, I'm looking for these kind of people, tell

9   me how many you have in your database so we can

10   analyze the data and determine how many people we

11   have that fulfills that particular requirement, so

12   that in essence is Naviant's business model.

13   Now, why do we do all this? What purpose

14   does it serve the business community? There are

15   many. I've just noted three here that I thought

16   might be meaningful to you.

17   One is we provide the data back to the

18   registration client with the enhancement of the

19   data attributes that we've associated so the

20   registration client has some view of who is buying

21   their products and services.

22   That's very important to the manufacturer

23   to know that because they -- since they distribute

24   through some intermediary, they are not in direct

25   contact with their customers.

128

1   So we would provide that back to the

2   registration client, and the registration client

3   would say, Gee, we have this kind of person buying

4   this model of computer, how can we find more of

5   those kinds of customers and launch marketing

6   campaigns to increase and enhance our business. So

7   that's the way a registration client would tend to

8   use this data is to find more like customers.

9   Another way they would use the data is say,

10   This particular product is being bought by

11   individuals that have these demographic

12   characteristics, so how can we fine tune our

13   advertising so that we are visible, more visible to

14   individuals with these kind of characteristics, so

15   it's used for a variety of purposes by a

16   registration client in order to improve the

17   efficiency of their marketing effort.

18   Another example would be a bank. Banks

19   love to promote their Internet banking packages and

20   capability because they can provide enhanced

21   service to their customers at a reduced cost for

22   those of us who sign up for Internet banking.

23   So a bank will come to Naviant and say, We

24   really would like to promote our Internet banking

25   capability, but we have a problem, we have no idea

129

1   in our customer base who is on the Internet and who

2   is not on the Internet, and really rather than do a

3   mass mailing to all of our customers, we would like

4   to do some selection.

5   So they would come to Naviant and say, If

6   we give you a list of our customers, can you match

7   those names against the names in your database and

8   tell us which ones of those are Internet enabled,

9   and we provide that service.

10   And then the bank can then target or

11   deliver a marketing campaign only to those

12   customers who are Internet enabled, and they might

13   even refine that further. They might refine it by

14   an age group or income level, but the primary key

15   for the bank, if they're promoting their Internet

16   banking package, is to only target to those that

17   can actually use that product or service.

18   A third example would be a retail dot com.

19   A retail dot com wants to drive traffic to their

20   web site, and you know you can always buy a

21   billboard on Highway 1 or you can by an ad for the

22   Super Bowl, but what they would want to do is to

23   work with Naviant looking for a particular type of

24   customer or individual that meets the selection

25   criteria and then do a direct mail campaign to

130

1   those customers with some kind of marketing offer

2   that would drive them to their web site so they

3   could offer a product or service.

4   Thank you.

5   MS. LANDESBERG: Thanks very much, Win.

6   Our next speaker is Peter Corrao. Peter is the CEO

7   of Cogit Corporation. Before joining Cogit.com, he

8   was Division President of National Accounts

9   Marketing for ADVO and the owner and operator of

10   Sports USA.

11   Peter?

12   MR. CORRAO: Well, thank you very much for

13   inviting me here today. Even though I come from

14   one of the largest direct marketing firms in the

15   country in ADVO, my comments today will mostly be

16   related to online marketing and its applications.

17   So I would like to talk to you today about

18   the developing science of visitor relationship

19   management and how it's applied on the web.

20   Before I do that, though, let me tell you a

21   little bit about the dilemma in commerce today on

22   the Internet. My company, like many other dot

23   coms, is a highly capitalized, venture capitalized

24   company. We've taken around $50 million in

25   investment to date and have yet to turn a profit

131

1   with our company. We look similar to others that

2   are out there.

3   The Internet commerce dilemma can be

4   summarized pretty much on the slide that I've shown

5   you here. There's two ways in a B-to-C environment

6   that companies are making money or trying to make

7   money on businesses on the Internet today.

8   One is content sites, and they're heavily

9   required or exclusively required, excuse me, to

10   bring advertising in, so their model is all about

11   advertising. They deliver free content to

12   consumers. They put advertising up for sale. They

13   sell that advertising, and their business model is

14   developed around that.

15   The other side of that is the commerce

16   sites, who are the E-tailers or retailers that are

17   trying to sell their goods and services online, and

18   theirs is a simpler model in that they're trying to

19   gather customers, turn those customers into

20   repeatable revenue.

21   Here's the dilemma. The Internet today

22   isn't very efficient, even with the tools that are

23   being applied to it. Imagine that you bought

24   133,000 banner ads, and you paid around $15 a

25   thousand for it, which would be the current going

132

1   rate if you had a media buying firm dealing with

2   either direct companies or with providers of those

3   services.

4   Of those ads that you bought out there,

5   around $15 a thousand, you would have earned

6   probably in the range of 300 visitors or so, so ads

7   saying 300 visitors clicked through from those ads

8   and came to your site to look.

9   Of those only five took action, so you're

10   getting started with the 133. Now you're left with

11   five that took action, and if they did take action,

12   only 20 percent of those, or one, would return

13   within the next year to buy anything from your site

14   again.

15   So just think of it from its most simplest

16   format -- and you're only dealing with the

17   advertising and attention components of being an

18   Internet company, your acquisition cost for a loyal

19   customer in this model is $2,000.

20   So the imperative here is that the Internet

21   has got to learn to be better and more focused on

22   how it brings -- on how it brings its clients in.

23   Let me show you a little bit about visitor

24   relationship management and why it's important.

25   Merchants want to increase desired action and get

133

1   consumers to buy things and services from their

2   site. Consumers want meaningful things to be shown

3   to them.

4   Merchants again want to display relevant

5   content to their customers. Consumers are

6   demanding instantaneous and ever faster access to

7   relevant content. Doing that is expensive.

8   Merchants want to optimize customer visits

9   and generate sustainable profits. Consumers expect

10   free Internet, other than access, or inexpensive

11   services at significantly discounted prices often.

12   We think that visitor conversion is critical to

13   making this model sustainable on the Internet.

14   What Cogit does is capture registration

15   information, I'm giving an example of what we do

16   here, with and amongst our customers. We match

17   that registration information then to available

18   data in the offline.

19   We have two data sources primarily. One is

20   Equifax Corporation, which we use their own bulk

21   data, and the other as of March 31 will be Claritas

22   data, which will be entered in our file at the end

23   of this month.

24   When that information is matched, we

25   irreversibly discard any personally identifiable

134

1   information that we found on the consumer, so if

2   you registered by name, we get rid of the name,

3   replace that with a random ID, and that random ID,

4   we can't go backwards and reengineer to find out

5   who that consumer is.

6   We generate then an anonymous profile on

7   that particular consumer, and then we allow our

8   customers to, one, know who's visiting their site

9   if they're not a customer yet, and, two, target

10   them with relevant content that will then incent

11   them to want to buy.

12   We think privacy is a big piece of doing

13   this. Consequently our profiles are 100 percent

14   anonymous. We think consumer PII shouldn't be

15   stored and used for further personalization. We

16   don't -- our visitors in the Cogit model are never

17   tracked across sites, so we only know what you're

18   doing on a specific site that you're dealing with.

19   Information from one client is never shared

20   with another. Behavior information is

21   never appended to our profiles, so the fact that

22   you bought something on one of our customers' sites

23   isn't appended to further your profile.

24   Clients aren't allowed to store Cogit's

25   returned data, and we semiannually have our web

135

1   site audited to validate that everything that we've

2   got in our web site is, in fact -- in our policy

3   is, in fact, what we do. Ernst & Young does that

4   audit. We were the first cyber audit that they did

5   and first audit attestation that they did.

6   So the notion is from a visitor

7   relationship management standpoint or knowing who

8   comes to your site so you can do something about

9   it, we think that that's critical to being able to

10   sustain the Internet commerce that's having trouble

11   sustaining itself today.

12   We think that convenient and relevant

13   information for consumers is what they demand and

14   what they want. Most of that information is given

15   to the consumer free today, although it's given

16   free against a model that is not panning out from a

17   general business model standpoint, and we think

18   that there's an optimum balance between

19   personalization and privacy.

20   We think we've come up with a method of

21   doing that and one that doesn't offend the consumer

22   and their ability to do it but yet does give the

23   tools needed to the sites so that they can continue

24   to make money in their commerce sites and/or money

25   in their content sites.

136

1   So thank you.

2   MS. LANDESBERG: Thank you, Peter.   Our

3   next speaker is Johnny Anderson, President and CEO

4   of Hot Data doing double duty for us today.

5   MR. ANDERSON: Thanks, Martha.   I wanted to

6   take a second and kind of look at a higher level on

7   how companies interact with customers and what are

8   the analytic and customer relationship management

9   applications that are driving a lot of the demand

10   for third-party information.

11   This really depicts a pretty typical

12   architecture of a CRM application that any marketer

13   would use one or more components of.   At the bottom

14   what you see is customer touch points.   That's how

15   businesses will either get information from their

16   customers and prospects or communicate with them.

17   So on the left-hand side you see kind of

18   the outbound communications media that a business

19   will use to communicate directly with the customer.

20   This is not TV and radio ads and so forth, but

21   they'll really use kind of Email, direct mail and

22   maybe some telemarketing either from an in-house

23   organization where they have their own telesales

24   organization or a contracted organization.

25   And on the right, what you will see is

1   really the way that people get information and then

2   sometimes communicate with their customers, and

3   that would be kiosks, which is kind of a new

4   emerging way to communicate with customers. You're

5   starting to see kiosks in, of all places, baseball

6   parks where the San Diego Padres have a customer

7   loyalty program.

8   And a customer puts in their preferences

9   when they sign up for the customer loyalty program.

10   When they visit the ball park they'll get the 10

11   percent off coupon for a specific restaurant that

12   happens to be in the area.

13   In-house or in-store communications, and

14   we're now starting to see companies even like food

15   chains implement customer loyalty programs where

16   transactions are tracked so that customized offers

17   and customized coupons can now be delivered to a

18   specific consumer.

19   Call center being somebody is calling an

20   800 number and talking to a customer service

21   representative, either a sales rep or a support

22   representative, and then obviously the web as one

23   of the major ways that customers are getting

24   information about products and services that a

25   company may offer.

138

1   It is a web visit where they may fill out a

2   form that says, "Send me more information," and so

3   that companies are getting some explicit

4   personalization type information that says, If I'm

5   going to a dot com or another sports kind of web

6   site, I'm going to check that I'm interested in

7   golf, so send me some golf information.

8   That's really stored in an operational data

9   store that's used for day-to-day kind of activity.

10   That's the data store that a CRM system may use so

11   that sales reps and a call center get access to a

12   customer record when an inbound call comes in.

13   They may have some transaction information, maybe

14   used for actually back-end processing where order

15   fulfillment takes place, but it's the data store

16   that's being used on a day-to-day basis.

17   Some companies actually will have a

18   separate data store that is used for data

19   warehousing and the analytics, and that information

20   is transferred back and forth with some

21   synchronization, extraction, transformating and

22   loading where a lot of information is both

23   rationalized, and that is, Bill Smith is also

24   William Smith and Bill Smith came in through the

25   Web and William Smith called in on a call, and that

139

1   information is rationalized.

2   And then the analytical tools at the top

3   are the things that are really driving a lot of the

4   marketing automation pieces, and that's things like

5   campaign management. If I understand who my target

6   audience is and who my best customers are, let me

7   generate a campaign and plan that campaign and

8   implement that campaign and then manage the results

9   from that campaign.

10   RFM analysis has been talked about already.

11   That's really understanding recency, frequency and

12   monetary transactions on a per customer basis,

13   really to understand who my best customer is, and

14   then to clone that customer and find more that just

15   look like them or be able to recognize them when

16   one of those comes into one of my touch points.

17   Category management's driven from that, and

18   that's really driving product synergies so if

19   somebody buys a particular product, they know,

20   through doing some category management analysis,

21   retail analytics, that a customer is likely to

22   purchase an additional product.

23   And then that starts to drive a lot of the

24   tools that marketing managers use to understand

25   their business, and those are things like data

1   visualization, being able to look at customer maps

2   for drive time analysis and trade area analysis;

3   reporting, so aggregate reporting on a per product

4   or per customer segment or per campaign

5   performance, and then other kinds of data mining,

6   being able to mine data that's transactional and

7   maybe inventory management type applications and

8   merging that kind of piece together.

9   Where Hot Data fits is really on the left

10   side of the equation, and that is we provide a set

11   of services that offer data quality and enhancement

12   of those databases, whether that's an operational

13   database or a data warehouse database.

14   The business models that are really in that

15   kind of space, and not just Hot Data related but

16   kind of industry wide, are really geared around

17   four sets of services. Marty mentioned address

18   data quality, and that's a big part, not only in

19   the real world, but also on the electronic commerce

20   side of being able to verify that an address is a

21   deliverable address, that it is standardized to

22   Post Office standards so I get a better postal

23   rate, that I can manage the consumer's change of

24   address, i.e., the 20 percent of consumers that

25   move every year, that that can be tracked in a

141

1   database, and then geo-coding addresses so that

2   addresses can be looked at in terms of where people

3   live.

4   Data rationalization and standardizing,

5   that's understanding Bill Smith is William Smith.

6   Consumer data enhancement is enhancement of

7   demographic, psychographic, and business data

8   enhancement. The flipside for us is that we also

9   deal with business to business marketers.

10   In a broad sense this is the architecture

11   that we use. We house consumer household

12   information. We house carrier route information.

13   We have services that house standardization, area

14   code update changes and U.S. national change of

15   address.

16   We provide customer data integration

17   technology to our customer, to our customers who

18   are contractually bound to the privacy use

19   restrictions and viewing restrictions that we pass

20   along to them, and that really from one click of a

21   button they can profile a subset or their entire

22   database and do things like address standardization

23   and profiling.

24   This is kind of a bright real world example

25   of what one of our customers uses, and they're

1   really a wireless broadband provider that was

2   really looking for -- to really target market. I'm

3   sure a lot of DSL, everybody has probably got DSL

4   things in the mail, and when I did, I went to try

5   to sign up for it, and I was out of range, and I

6   couldn't sign up.

7   So they got me to respond, but they got me

8   to be hostile because I was outside the range, so

9   our customer really wanted to target people outside

10   10,000 foot radius from a central office, and after

11   having done some ideal customer profiling for them,

12   identified who their target should be and who their

13   ideal target should be in that particular

14   environment.

15   I am out of time, and the band's about to

16   start playing, so I'm going to turn it back to

17   Martha.

18   MS. LANDESBERG: Thank you, Johnny. Our

19   next speaker is Lynn Wunderman, CEO of I-Behavior,

20   also serving two roles for us today.

21   MS. WUNDERMAN: Actually, I don't know if

22   it's true, but I heard a rumor here today that the

23   real reason we've been asked to be here is that

24   we're being auditioned for participants on a new TV

25   game show. It's called "Database Marketing

143

1   Survivor," you know the one where they put a bunch

2   of database marketers in a room in Washington to

3   talk about their business models. Last one

4   standing wins a million dollars. Anybody else hear

5   this? I think I probably better keep my day job.

6   Anyway, I'm here to talk to you today about

7   a company called I-Behavior, and I founded this

8   company with my father-in-law, Lester Wunderman,

9   yes, there is a family relationship for those who

10   have asked, and we created this company largely

11   with the vision to bring a lot of the art and

12   science of traditional direct marketing to the web

13   and to new media.

14   Now, our formula is really very

15   straightforward. Everything that we do, the way we

16   manage data, the way we structure it, the way we

17   analyze it, all the products that we create from

18   data has its roots in a very simple but proven

19   principle we've known for decades as traditional

20   direct marketers. You've heard this theme a lot

21   today. Past behavior is the single, strongest

22   predictor of future behavior. It's no coincidence

23   that our name is I-Behavior.

24   Now, we take for granted gaining access to

25   behavioral information in direct mail. We can pick

1   up the phone. We can call a list broker, and we

2   can rent names from one of any 30,000 plus odd

3   lists based on what people bought, when they bought

4   it, how much they spent.

5   Can't do that today on the Internet. That

6   type of behavioral information doesn't exist. We

7   have interest categories. We have product

8   registration data, but not that level of

9   behavioral, experiential information.

10   Beyond that, what's been largely unexplored

11   is the opportunity to target and understand

12   consumers based on their multi-channel buying

13   behavior. Even though we know that a merchant's

14   multi-channel shoppers, the buyers, tend to be

15   their best customers, in fact statistics show that

16   they're worth an average of over 30 percent more

17   than their single-channel counterparts, and we know

18   that those customers that can master these tools

19   will be the multi-channel winners of tomorrow.

20   So to fill this gap in the marketplace,

21   we've created one of the first, if not some say the

22   first, cooperative database that truly combines

23   highly detailed, transactional information on and

24   offline on known direct channel buyers.

25   Now, before anybody starts slinging arrows

1   up here, I will tell you that there are significant

2   privacy safeguards built into this product, but

3   before I get to them, I want to make sure that

4   everyone has an understanding of the business model

5   so they have the context in which to evaluate them.

6   First of all, I mentioned earlier for those

7   of you who are not familiar with the concept of a

8   co-op database, it's created when marketers pool

9   all their customer names and related buying

10   behavior in order to gain access to names of

11   qualified prospects as well as additional data on

12   their current customers that would otherwise be

13   unavailable in the marketplace by which to build

14   their business.

15   Now, this is a proven business model in the

16   offline catalog industry. I'm sure you're probably

17   familiar with names of companies such as Abacus.

18   Experian has a similar offline product catalog

19   called Z-24.

20   The reason that these products are so

21   successful is really two basic things; number 1,

22   the superior performance of a list. The fact that

23   all this rich behavioral information goes in to

24   fuel the selections, they have significantly higher

25   response rates than the average mailing list,

146

1   outside mailing list, by which one would normally

2   have the opportunity to do prospecting in the world

3   today.

4   Secondly, in terms of their pricing, they

5   are offered to members, and by the way only members

6   have access to these names. You have to contribute

7   in order to get data out. Members get access to

8   these names at a preferred rate, virtually half the

9   price of a standard vertical list today.

10   So what we're doing at I-Behavior is we're

11   expanding this context so that beyond catalogers

12   we're including publishers, E-tailers, club and

13   continuity marketers, virtually anyone who does

14   direct-channel marketing, and we're creating it in

15   a way that's a true multi-channel vehicle so that

16   you can target more efficiently the Email and

17   postal mail today. Tomorrow it will incorporate

18   wireless, interactive television and virtually all

19   forms of addressable media.

20   Now, there are two reasons why marketers

21   want to gain access to the data. The first and

22   most obvious is prospecting, and certainly you can

23   see by the way that we consolidate information

24   across marketers, across channels, we have a much

25   more complete portrait of these shoppers, their

1   buying patterns and their value.

2   This thing is bigger, smarter than any

3   single marketer could ever create on their own.

4   That's because when we take data in from a

5   merchant, we get it down to each transaction, the

6   entire shopping basket of a person's purchases so

7   that we can collect all the rich recency,

8   frequency, monetary value information we've been

9   talking about earlier today as well as we also get

10   one component that's generally not been available

11   in co-op databases previously.

12   Instead of just giving to each marketer who

13   participates, to all their transactions, some high

14   level general category associated with the affinity

15   for that particular property, we actually get item

16   level data so that we know exact products down to

17   the SKU level that an individual is buying, and I

18   can tell you that that is incredibly powerful

19   information from a predictive standpoint when

20   you're looking for those subtle predictive patterns

21   in the data for those kinds of tools that we were

22   talking about earlier today.

23   Now, we have proprietary technology that

24   allows us to create a common language across

25   marketers that we can really leverage the value of

148

1   this product level information. We also have

2   proprietary technology that helps us link multiple

3   Email addresses back to a single individual and

4   optimize the match between the on-and the offline

5   data, but I'm not here to talk to you about some of

6   our competitive strengths. I really want to focus

7   on the business model itself.

8   There are two key features that I think are

9   inherent in the kinds of co-op you should be aware

10   of. First of all, this is the only place on the

11   Internet today where you are assured of not talking

12   to your own customers as prospects. That's

13   because, unlike in the traditional direct mail

14   community where mailers are really familiar and

15   comfortable with the process of sending their files

16   to a compiler -- I'm sorry, to a reputable service

17   bureau, I see I'm getting short on time here,

18   whereby they can exchange their names, they can

19   unduplicate them, you can suppress out your current

20   customers, we already know who your customers are

21   because we already have them in the database.

22   Secondly, it's a closed loop process so

23   when we send an Email to someone about this

24   product, they may read the Email. They may not

25   respond to that particular communication, but if

1   they remember the marketer and two or three weeks

2   later they have a particular need, they go to the

3   Web site and they buy, we would know about that,

4   not because we're tracking anything in terms of

5   cookies. I don't want to get anywhere near that,

6   in terms of your surfing of the Web, but we know

7   because the merchant sends us back their data.

8   We match that back to our contact history.

9   We get smarter about targeting you the next time

10   around in the future, even if we don't get credit

11   for that response, because we maintain a

12   professional history on the file.

13   Now, the fact that we maintain a promotion

14   history is really of true benefit to both the

15   consumer and to the merchant. First of all, it

16   allows us to identify habitual non responders.

17   That's very important. Don't want to keep mailing

18   to people who don't want to purchase from you.

19   Secondly, we keep tabs on any correlating

20   between the volume of mail so we can look at your

21   individual saturation rate and any negative

22   correlation against response.

23   Now, the second way that mailers want to

24   gain access to this database is to be able to

25   target their own and mine the value of their own

1   customers. Now, we can do that to help them expand

2   it into new categories, to reactivate lapsed

3   buyers, to turn their offline buyers to more

4   efficient online buyers.

5   So, for example, if an apparel merchant

6   comes and says, "We're expanding into swimwear,"

7   and they may say, "I want to target everybody in

8   own our file that has bought from us in the last

9   12 months, who has bought swimwear from any other

10   merchant in your database. We'll create a one time

11   file, do a one time mailing. Anybody who responds

12   to that mailing, they own the rights to that data.

13   But we will not append any information

14   permanently to that marketer's files, not an Email

15   address, not a transaction because we don't have

16   marketing rights, and there are privacy issues

17   attached to that.

18   What we will append on an ongoing basis are

19   model scores. Remember from our discussion

20   earlier, it's nothing more than a mathematical

21   probability. I have a .8, you have a .4. I'm

22   twice as likely to buy swimwear as you are. Even

23   if we have the same score, you don't really know

24   what it is in terms of personally identifiable

25   information that got us there because it's a

1   formula, and it's made up like a Chinese menu. I

2   got there because of age and income. You're there

3   because you just bought shoes over the Web and you

4   have kids. We don't necessarily have the same

5   profile.

6   I will also say that there's some other

7   creative ways to use these tools. In fact you can

8   use them to serve up dynamic content right on the

9   Web site to register users.

10   Now, I promised you that we would talk

11   about privacy, and I just want to say that in terms

12   of the offline data, we follow the industry

13   standard which is opt-out for direct mail

14   solicitations. We're not looking to reinvent the

15   wheel in direct marketing from that standpoint.

16   All of our member companies actively notify the

17   people who buy from them that they share data with

18   trusted third-parties.

19   If they choose not to do that, they send a

20   request to the merchant. That data comes back to

21   us in one of their updates, and that information is

22   removed in the course of our database build.

23   However, online is a different animal, and

24   we know that people have different expectations

25   from a privacy perspective online. We respect

152

1   that.   We've been extremely proactive on the

2   privacy front going what we believe is really above

3   and beyond today's best practices in industry

4   standard.

5   First of all, this is a double opt-in

6   database, so in other words, no consumer will be

7   targeted for an Email communication unless they

8   raised their hand, self selected, and said they

9   actively agreed to participate. When they do, we

10   allow them to tell us the maximum number of Emails

11   that they're willing to receive in any time period.

12   We will not exceed that. We give them

13   access and control to the aggregated level of

14   information that we utilize for selections, so they

15   can come in, request a copy of their profile. They

16   can say, "Don't use this Email address, use that

17   one. I know I bought sports equipment in the past;

18   but you know what, that was just a gift, please

19   don't send me any more sports offers." Obviously,

20   they can opt-out at any point in time.

21   I will also tell you that we do not allow

22   marketers to cherry-pick this file. They can not

23   come in and say, We want people of this age and

24   this income who bought these products in this time

25   frame." Not online, because as far as we're

153

1   concerned, anyone who would respond to that kind of

2   an offer, you could attach that purchase history

3   and that profile of the individual and you would be

4   releasing personally identifiable information, and

5   we don't think you should do that.

6   So we work with the marketer to understand,

7   What's the product you're selling, what's your

8   price point, what's the promotional nature of your

9   offer. We construct targeting tools, create a

10   composite score, rank them on the database. All

11   you know is these people had a score of .75 and

12   above. That's nothing in terms of personally

13   identifiable information.

14   Finally, we do not release any of the data

15   on this file to -- no addresses -- to anyone for

16   any purpose beyond a reputable service bureau

17   offline. They go seemlessly through our own

18   service bureau online. They never get access to

19   the data.

20   I will also tell you that we took this

21   concept into consumer research. We told them what

22   kind of data we have, how it benefits them, what we

23   do with it, what we don't do with it, and they were

24   not only very positive about the concept, they

25   actually embraced our privacy policies.

1   So, in summary, I just want to say that we

2   have a proven business model in terms of the

3   behavior-based co-op, which has been expanded to

4   meet the unique needs of multi-channel marketers.

5   We have superior technology and a level of data

6   that helps us generate superior behavior

7   predictions at a good value to our clients, and

8   we're doing it in a way that we believe respects

9   consumer privacy and is looking to set new

10   standards in that area.

11   Thank you.

12   MS. LANDESBERG: Thank you, Lynn.   The last

13   speaker on our panel today is Jerry Cerasale,

14   Senior Vice President for Government Affairs at the

15   Direct Marketing Association.   Jerry joined the DMA

16   in January 1995 and is in charge of the DMA's

17   contact with Congress, all federal agencies and

18   state and local governments, a very busy man.

19   Thanks for being with us.

20   MR. CERASALE: Thank you, Martha.   Lynn,

21   just so you know, for this panel, I'm the last one

22   standing, so send the check.

23   Before I get to my slides, I wanted to

24   just, first of all, thank the FTC for having me

25   here and for having this workshop.

1   I wanted to make three quick points. The

2   first is that the information that we're talking

3   about today is marketing information, information

4   that's used to send you a solicitation, an offer

5   for something. It's not being used to give you

6   employment or refuse employment or anything of that

7   sort or for insurance, whether or not you're

8   eligible for insurance and things like that.

9   In particular as well, just to get on a

10   topic that was raised, DMA guidelines would also

11   say that information that comes from a doctor-

12   patient or medical provider-patient relationship

13   should be only on a consent basis, and that's

14   pretty well standard within the industry as far as

15   we know.

16   Second, the information that you gather is

17   basically to send a solicitation about a particular

18   product, so it only goes once. It's a one-time use

19   that people use to try and find new, prospective

20   clients.

21   And third is that, generally speaking, the

22   information doesn't go to the marketer. What you

23   receive is, the information goes to a service

24   bureau that is either sending out -- making phone

25   calls or sending out the mail pieces and then

156

1   returned back to the -- it's not used again, so

2   it's that kind of information that we're talking

3   about.

4   Martha asked me to talk specifically about

5   prospecting and why we do it and how is it used, so

6   I wanted to use because of my -- to make it simple

7   so I could understand it, use some hypotheticals,

8   and if Allison gives me time, I'll go to some more

9   specifics after the hypotheticals, depending how

10   nice she is to me.

11   The first is the idea of a new company. I

12   just started something, I have a brand new idea.

13   Think about Marty's view when he had the list of

14   what marketers have and what compilers have. He

15   said marketers have information on their customers.

16   Well, I'm brand new. I haven't got

17   anything. I have no customers, nothing. I have a

18   new idea for a new golf club, so what am I going to

19   do? And the other thing is I'm going to sell it

20   over the Internet. That's what I want to try and

21   do. So what do I do?

22   Well, I'm going to go to a golfing magazine

23   likely and try and see if I can rent the list,

24   because those are people I would assume would be

25   interested in golf, and I'm going to use this list

1   to mail it because I'm starting to find -- and

2   we're starting to find that mail, snail mail is

3   being used successfully to drive customers to Web

4   sites to make sales.

5   We find that from our catalogers and so

6   forth, that it is a very important piece tool in

7   E-commerce or multi-channel marketing. So, this is

8   what I want to do so.

9   So I go and get the golfing magazine list,

10   and it's one million names, and that is

11   outrageously expensive to send, so I can't do it,

12   so I want to go -- I go to an information compiler,

13   and I say, Look, I would like to have some more

14   information from an information provider, I want to

15   try and narrow this list down.

16   I think that maybe this piece would likely

17   be best suitable for women. I think that it may be

18   for women probably over 40 because it helps give

19   distance, and if you really swing hard it messes up

20   the way the ball goes, so I think that that's what

21   I want, and I know that likely I think that it's

22   expensive, higher income, let's see if I can get

23   that from Census data.

24   I'm selling it over the net so I want to

25   use Win's stuff to make sure they're Internet-

158

1   enabled, and I think maybe five miles from a golf

2   course. Let's just pick these out of the air.

3   Maybe we can get these things, and it finally comes

4   down to 500,000 pieces, people that I can send this

5   to, and that's within my budget, and that's what

6   I'm going to use, and that's how a marketer can try

7   and prospect a new start-up business.

8   Without the information from third parties,

9   I can't start. I cannot start a catalog. I cannot

10   start driving people. I can try, put it up on a

11   Web site, see if search engines get me some people,

12   but that's not going to be a viable economic model.

13   Another idea for prospecting is a current

14   marketer looking for new customers. The idea I'm

15   trying to use here, I'm selling books and probably

16   I'm selling books online, I'm trying to use online

17   and offline because this is supposed to be online

18   and offline information so these are my examples.

19   And I know because I sell books that

20   they're upper income, they're Internet-enabled and

21   these people that purchase from me happen to be

22   people who live more than 20 miles from a book

23   store and more than a hundred miles from a discount

24   book store, so that's my marketplace of my current

25   set of customers.

159

1   40 percent of Americans never purchase

2   remotely. 60 percent of Americans do, so I want to

3   try and reach some new customers, so I'm going to

4   go and try to find information that matches that

5   market because it works for me today, and I'm going

6   to send a mail piece to them.

7   I may in fact ask for a split on this test,

8   people who have purchased, those that were in the

9   60 percent piece of the pie, and those in the 40

10   percent that have never purchased, to try and see

11   if I can reach new customers differently through

12   this mail piece, and so I send it.

13   This is what I want. This is the

14   information I asked for. The information provider

15   supplies a list to the letter shop I'm going to

16   use. They send it out. They make sure the current

17   customers are deleted. They use hopefully the DMA

18   mail preference list, and they prepare the pieces,

19   and they send them out.

20   I never see the list. I only know someone

21   was on the list if in fact they come back and

22   purchase from me. Then I would know that they

23   responded, so that's the only way it happens, and

24   that's generally how you use prospecting data.

25   That's to try and find someone new. You know from

    1   past behavior or you have a guess, if you're brand

    2   new. You don't have any past behavior in your --

    3   on your product. You make a guess: We think this

    4   is what the market is for. That's how we use the

    5   prospecting.

    6   Now, let me give you a couple of quick

    7   examples of real life things that have been

    8   testified, to the process has been in Congress, in

    9   testimony before Congress. One company is Grolier.

   10   It's no longer in existence. It's been bought out,

   11   but Grolier is a bookseller selling things remotely

   12   out of Danbury, Connecticut, and it basically sells

   13   to children, basically sold discounted Dr. Seuss

   14   books.

   15   The market for this company was rural

   16   Americans who lived more than 50 miles from a book

   17   store, families that had young children and were

   18   low income. The only way for Grolier to find these

   19   people to give them books that their children can

   20   read or books that they could read to their

   21   children was to have information to find them, so

   22   it was necessary to have a free flow of

   23   information.

   24   And marketers -- the other is stylists, an

   25   after-market automobile company that sells after-

161

 1   products for minivans, seat belts that can be

 2   adjusted better for children, back-up warnings on

 3   minivans, so their market, families that own

 4   minivans that have children that are outside of car

 5   seats, to try to give them an offer of some safety

 6   to add to their cars, and that's the market, and

 7   they needed the information to try and find it.

 8   One of the things that I want to make sure

 9   that you also know, my time is now up, I did get

10   through the two examples, thank you, I didn't get

11   my million dollar check yet though, but the one

12   thing that the DMA says, you have to tell people

13   that you share information with third-parties and

14   give them an opportunity to say "no."

15   And that's really the basis, that people

16   who take the information and share with

17   third-parties have to tell you that they do that,

18   and to be a member of DMA you must do that.

19   Thank you for the time.

20   (Applause.)

21   MS. LANDESBERG: Well, we have just a very

22   few minutes for questions from the audience. If

23   you would raise your hand, and if do you have a

24   question, we'll bring the mike to you.

25   MR. HENDRICKS: Two quick questions. Evan

162

1   Hendricks, Privacy Times. In the offline world, a

2   lot of times people want to know when they receive

3   a mailing, "Where did you get my name?"

4   Aren't there a lot of instances where

5   there's contractual language that prevents

6   organizations from disclosing that? That's the

7   first question.

8   And the second question is I assume that

9   the 20 licensees of the NCOA sell new movers' lists

10   which they're able to produce because of the data

11   they get from NCOA, but do other companies also

12   sell new movers' lists?

13   MR. ANDERSON: I'll answer the NCOA

14   question, and one of the restrictions that we have

15   from the USPS is that we specifically cannot

16   generate new movers' list, so this is specifically

17   -- our NCOA services are specifically for people

18   that are in a database, but we will not, cannot

19   contractually generate a new movers' list that can

20   then be sent out to marketers that are interested

21   in people that have just moved.

22   MR. HENDRICKS: How are they generated,

23   where they're moving?

24   MR. ANDERSON: A lot of other different

25   sources, but none of which come from the USPS.

163

1   MR. ABRAMS: In terms of the question

2   about, "Where did you get my name?" Increasingly

3   during the 12 years that I was with an information

4   aggregator, the contractual arrangements that

5   limited the ability of the marketer to say where

6   the name came from began to disappear from the

7   marketplace.

8   And increasingly organizations are

9   acquiring data from organizations that have given

10   notice, and organizations that even if they say,

11   "No, you can't tell them where the data came from"

12   they say "Pass on the name to us and we will call

13   the individual and let them know that we were the

14   source."

15   So while that was the norm ten years ago,

16   that norm has been changing over time.

17   MS. LANDESBERG: Jerry, did you have a

18   comment?

19   MR. CERASALE: I was going to just comment

20   specifically on the NCOA because actually there is

21   a contract, but no one can use that for marketing

22   purposes. It's just to correct mailing lists, to

23   increase the efficiency of the Postal Service, so I

24   don't have a lot of those letters.

25   MS. LANDESBERG: Other questions? All

164

1   right, then. Seeing no more questions, I would

2   like to thank our panelists for a wonderfully

3   informative session.

4   Thank you. If I could ask you just to bear

5   with us for a moment, we'll go straight into the

6   next session -- so don't go anywhere.

7   (Discussion off the record.)

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

165

 1   SESSION 4: HOW DO MERGER AND EXCHANGE AFFECT

 2   CONSUMERS AND BUSINESSES?

 3   JESSICA RICH, Assistant Director, Division of

 4   Financial Practices, FTC, Moderator

 5

 6   PANELISTS

 7

 8   FRED CATE, Professor of Law and Harry T. Ice

 9   Faculty Fellow, Indiana University School of Law

10   JASON CATLETT, President, Junkbusters Corporation

11   JERRY CERASALE, Senior Vice President, Government

12   Affairs, Direct Marketing Association

13   MARY CULNAN, Slade Professor of Management and

14   Information Technology, Bentley College

15   EVAN HENDRICKS, Editor/Publisher, Privacy Times

16   RICK LANE, Director, eCommerce and Internet

17   Technology, U.S. Chamber of Commerce

18   GREGORY MILLER, Chief Privacy Officer and Vice

19   President of Corporate Development, MEconomy, Inc.

20   BRIAN TRETICK, Principal, eRisk Solutions, Ernst &

21   Young

22

23

24

25

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025

166

```
 1                       SESSION FOUR

 2            HOW DO MERGER AND EXCHANGE AFFECT

 3                 CONSUMERS AND BUSINESSES?

 4               -    -    -    -    -    -    -

 5            MS. RICH:   Hello.   If everyone can take

 6    your seats again, please.   We're going to start

 7    this next panel.   I'm Jessica Rich.   I'm an

 8    Assistant Director in the Division of Financial

 9    Practices here at the FTC, and I'll be moderating

10    this fourth panel, which will focus on the effects

11    of merging and exchanging consumer data on both

12    businesses and consumers.

13            In other words, how do consumers and

14    businesses benefit from these practices and what

15    concerns, if any, do these practices raise.

16            I think we've heard some references to the

17    various ways in which people benefit or some of the

18    concerns that people have, but we're trying to

19    drill down and talk more specifically about this

20    particular topic.

21            We have a great group of panelists for this

22    session.   We're going to start with brief

23    statements from each of them, three minutes each,

24    and we're going to hold everyone to that, but I

25    don't want to be too -- everyone has been great
```

167

1   about keeping to their time, so I probably don't

2   have to lecture them too much.

3   Then we'll have a discussion among the

4   panelists so we can examine the issues in greater

5   detail, and we'll hopefully have time for

6   questions. I think for this panel questions are

7   fairly important, so at about 3:15, if you're in --

8   get ready to ask some questions if you're in this

9   room, and if you're in one of the overflow rooms,

10   please come up to the door here so we can give you

11   a microphone to ask your question.

12   I want to emphasize that this is a long

13   panel, and it's easy to focus on a lot of different

14   topics, but we really want to focus on the effects

15   of the particular practices we're talking about

16   today, which is the merger and exchange of consumer

17   data, the effects on consumers and businesses, that

18   specific topic.

19   We're going to let our speakers go

20   alphabetically. I think they may be seated

21   alphabetically, and we're going to start with Fred

22   Cate, and I'll introduce him. He's a professor of

23   law and Harry T. Ice Faculty Fellow and Director of

24   the Information Law and Commerce Institute at the

25   Indiana University School of Law in Bloomington.

168

1   He also serves as senior counsel for

2   information law with Ice Miller Legal and Business

3   Advisors and is a visiting scholar at the American

4   Enterprise Institute. He specializes in privacy

5   and information law and appears regularly before

6   various legislative committees and professional

7   groups on these matters.

8   Fred?

9   MR. CATE: Great. Thank you very much, and

10   thank you also for the opportunity to be here.

11   I've tried all morning long to condense

12   this to three minutes, and I think I've got it now,

13   so let me just make two points. I'm just going to

14   take up one of the questions that was asked, and

15   that is the impact on consumers, and let me talk

16   about just briefly two points.

17   One of them is the use of information to

18   overcome the obstacles of market size and distance

19   to make it possible to deliver customer service,

20   customized service and personalized service to

21   customers, and there are many examples of this,

22   such as better targeting of what is stocked in

23   stores.

24   We've already heard about better targeting

25   of the type of mail or commercial offers that are

169

```
1    sent into homes, more accurate decision-making

2    about customers, about consumers who come seeking

3    service, greater convenience for consumers in many

4    ways all the way from having forms pre-filled in,

5    one call service center being able to change your

6    or address in multiple accounts with a single call,

7    loyalty programs.

8         I think frequent traveler programs are

9    something we almost all share in common at least in

10   this room, or returning goods without a receipt.

11   These are exactly the types of examples of, if you

12   will, sort of overcoming the type of problem that

13   large, diverse and particularly online markets

14   pose.

15        The second, I think, set of examples of the

16   real impact on consumers is where we see

17   dramatically new and different types of benefits,

18   and maybe the best example is lower cost, and this

19   is one area in which there's been a fair amount of

20   studies completed recently showing, for example,

21   Mike Turner's study, a billion dollars in the

22   retail apparel industry in cost reduction by the

23   ability to use personalized information, Walter

24   Kitchenman's study showing $85 to 100 billion in

25   annual savings in the mortgage credit market
```

1   because of access to personalized information, the

2   Staten and Barron Study showing $150 billion

3   annually in non mortgage credit, the Ernst & Young

4   study, Ernst & Young will be speaking later, $17

5   billion a year focusing just on 30 percent of

6   financial services companies.

7   The point is this consistent evidence from

8   these studies about the way in which the use of

9   personalized information saves consumers money, but

10   there are other good examples, either dramatically

11   new and different services, for example, the wider

12   availability of products and goods and services.

13   I don't mean simply expanded access to

14   credit, although we have studies clearly

15   demonstrating that, but even the points made on the

16   earlier panel about the way in which a business

17   operates, the way in which AOL got started by

18   sending out floppy disks to people who had

19   computers (and identifying people who had computers

20   of course was key to that strategy), and finally

21   the more apt, rapid and efficient, more accurate

22   fraud detection and prevention.

23   I think one thing that almost anyone who

24   works in that field will say is that personalized

25   information is the key to detecting and preventing

171

1   fraud. If you don't have access to it, you'll lose

2   one of those key tools.

3   Thank you.

4   MS. RICH: Next we have Jason Catlett.

5   He's President and Founder of Junkbusters

6   Corporation, a computer scientist with a Ph.D. in

7   data mining. Dr. Catlett has worked on issues

8   relating to the interplay between technology,

9   marketing and privacy at such places as AT&T, Bell

10 Laboratories, the University of Sydney and various

11 other academic settings.

12   In addition to academic publications, Dr.

13 Catlett has contributed articles to such

14 publications as the Privacy Journal and Direct

15 Marketing News.

16   DR. CATLETT: Thanks very much, Jessica,

17 and thanks again to the Commission for inviting me

18 today.

19   First let me put a concern to rest of Jerry

20 and anyone who feels like they're on a survivor

21 program, or Commissioner Swindle, that I'm not

22 going to be posting any profiles of people. I did

23 go through an exercise that you can read in the

24 handout out there of asking people if they would be

25 willing to have their profiles posted and then

172

1   going to companies to actually see the profiles

2   that the consenting data subjects have.

3   Unfortunately, though I have a number of

4   volunteers, I have no company yet willing to place

5   on the table before us a real profile, which I

6   think is regrettable.

7   However, what I'm going to talk about today

8   is not that. It's three points. First, let me

9   state that Fred is absolutely right that the

10   benefits of information processing are enormous.

11   Let's remember, however, that the

12   overwhelming majority of those benefits come

13   without personally identifying information.

14   Wal-Mart is an extremely good example. It's all

15   about inventory and forecasting, and most of the

16   benefits come without PII.

17   Where you do use personally identifying

18   information, as Marty Abrams pointed out, the vast

19   majority of that is about personal information that

20   the business already has and not that it gets from

21   third parties.

22   Now, turning to the question of whether

23   direct mail actually reduces -- sorry, targeting

24   that information reduces the amount of junk mail

25   that people get, in fact it actually increases it.

                    For The Record, Inc.
                     Waldorf, Maryland
                      (301) 870-8025

1   If you look at the historical trend from say 70

2   billion direct mail pieces per year in the United

3   States, it's been trending up as the technology has

4   made targeting better and better.

5   We do see more offers that people respond

6   to. This is true, but the typical response rate

7   being in the low percentage figures as Michael

8   said, that results in a lot more junk, and Jerry's

9   example of the golf course magazine is a good one

10   here because without the information, a lot of

11   offers are uneconomical and would not be mailed.

12   So the additional information causes more offers to

13   be responded to, also causes more unwanted

14   solicitations because the information isn't

15   perfect.

16   Now, let me turn to some of the negative

17   aspects of personal information. One that we

18   haven't discussed yet, I think is important, goes

19   under the name of dynamic pricing or price

20   discrimination. The American public loathes the

21   idea that the person sitting next to them is

22   getting a lower price on the same goods that

23   they're getting.

24   They loathe the idea that I'm getting a

25   lower price than Fred is for example, and I think

1   Amazon learned this to their distress when it came

2   out that they were randomly, they said, pricing,

3   and Amazon very quickly stated that they would

4   never base price points on demographic information.

5   They said they didn't really have click stream

6   data. I would like to see a clarification on that.

7   I'll wrap up with my last point, which is

8   the effect on non-participation. I would dearly

9   love to see some figures that talked about the

10   impact on participation of profiling, but we don't

11   have those figures. We just have figures that

12   Forester put out last year of $12 billion lost in

13   online commerce due to privacy concerns.

14   But those privacy concerns were not

15   specified to the level of particular profiles where

16   the people were concerned about SPAM, or about the

17   actual nature of the profiles. We simply do not

18   know.

19   I'll leave it at that.

20   MS. RICH: Great. Jerry Cerasale is next.

21   He was just on the previous panel, but I'll remind

22   you that he's Senior Vice President of Government

23   Affairs at the Direct Marketing Association.

24   MR. CERASALE: On this panel, still looking

25   for my million dollars, but whatever, I wanted to

1   just take a look at that study of restriction of

2   data that was released yesterday and just raise to

3   you that it's a billion dollars in just the apparel

4   area, but there's an additional study that's an

5   overlay on it that says that the individuals -- the

6   groups that purchase apparel remotely to a greater

7   extent, a greater proportion than their density in

8   the population, are rural Americans and

9   economically disadvantaged intercity, the people

10   who are not adequately served by brick and mortar

11   retailers, the people who don't have other choices,

12   who end up paying a disproportionate share of any

13   restrictions, cost of restrictions on privacy.

14   Those who have the fewest choices are the

15   ones who pay the most based on that study.

16   I want to add to what Fred had said. What

17   we know is that the sharing of information helps

18   reduce fraud. We've seen studies where fraud,

19   credit card fraud over the net in Europe is twice

20   as great as that in the United States. We can

21   attribute that in part I guess because we're more

22   honest than Europeans, but I'm not certain that

23   that is the full case.

24   The real reason is that part of the

25   restriction in Europe is you can't use information

176

1   collected for purposes other than the specific

2   reason that information was collected, so a billing

3   address on a credit card cannot be used for

4   anything other than billing.

5   So that in the United States, if you're on

6   the Internet or even on the phone, if you call or

7   want to purchase a good and here's the credit card

8   saying, I'm Jerry Cerasale, give them a credit card

9   number, and it's being delivered to the billing

10   address, that's fine.

11   In Europe they can't check that. In the

12   U.S. they can. If it's not going to the billing

13   address, I'm sending it to my mother or ostensibly

14   I'm sending it to my mother, they ask for the

15   billing address. If I can't give them the billing

16   address, then they figure it's probably not Jerry

17   Cerasale, so it's an added thing for fraud

18   prevention.

19   So information flow is important from that

20   score as well, giving benefits to people. There

21   are an awful lot of jobs, low income jobs. It's

22   interesting when you go on visits with senators and

23   representatives that they want direct marketers to

24   come with them to set up call centers, to set up

25   warehouses and so forth in areas where there are

1   economic downturn areas because they want to try to

2   build them up.

3   These are jobs that can be part time.

4   People can be trained fairly readily, so those are

5   advantages as well as choices to consumers. You

6   also have employees and the efforts there in trying

7   to do that.

8   It also allows for easy entry, easier entry

9   for new businesses so that you can get greater

10   competition. I do not have to build the store. I

11   can be L.L. Bean in my basement getting a list of

12   Maine hunters, Maine hunting licenses, out of state

13   people, sell 15 shoes, have to repair 14 of them,

14   but that's how I start a billion dollar business.

15   Those are the things that can happen and

16   happen readily with the sharing of information.

17   Thanks.

18   MS. RICH: Next we have Mary Culnan. As we

19   noted earlier, Mary is the Slade professor of

20   Management and Information Technology at Bentley

21   College in Waltham, Massachusetts, where she

22   teaches and conducts research on information

23   privacy.

24   MS. CULNAN: Thanks, Jessica. My point I

25   would like to make in my three minutes is that fair

1   information practices should apply to the merger

2   and exchange of consumer data, that is to

3   profiling, and it's not clear that it really does

4   today.

5   One way I think to close the trust gap and

6   the misunderstanding that Commissioner Swindle

7   talked about this morning is through much greater

8   transparency about how compilers and co-op

9   databases acquire personal information and what

10   they do with it.

11   There's some parallels here to the network

12   advertising model where in fact consumers do not

13   have a direct relationship with the compilers and

14   the co-op databases, and they frequently don't know

15   who these firms are, so if they wanted to contact

16   them, they would not know how to start.

17   So what are some of the things that we

18   need? We need much more notice where data are

19   collected directly from consumers. I've never seen

20   a notice that says, "We share your name with

21   carefully selected companies or carefully selected

22   third parties and one of America's largest data

23   compilers."

24   And I think to the consumer in fact the

25   idea of a carefully selected company, while in fact

1   the information is being shared for marketing

2   purposes, that is not the same thing to the

3   consumer as you buy from L.L. Bean and you get a

4   mailing from Eddie Bauer or something like that.

5   So I think that all the compilers should

6   provide an easy way for people to opt-out, and

7   there needs to be a better way for people to be

8   pointed to the Web site or however the opt-out is

9   handled, and I think the companies that enhance

10   their customer databases should include this fact

11   in their privacy notices just out of fairness.

12   There are a couple questions that need to

13   be answered. What does opt-out mean for compiled

14   databases? Does my personal information stay in

15   the database? Is it still used for enhancement

16   purposes, or does it just mean that my name is

17   removed from the mailing list when people come to

18   get a prospecting list and it is just gone?

19   Should consumers be able to have their

20   personal information removed from a compiled

21   database? And then, second, the always popular

22   "What kind of access is appropriate?"

23   In conclusion, I think really there's a

24   need to bring consumers into the loop. What I hear

25   -- it strikes me a lot of it is "We know what's

1   good for you" is kind of part paternalistic because

2   most consumers are smart, and they make good

3   choices in their own interest when they have

4   information.

5   And I think access to personal information

6   is not an entitlement just because people don't

7   know about the compilers, and basically then they

8   don't know about it.

9   Consumers do benefit a lot from compiling,

10   and I think the marketing profession needs to

11   develop some effective strategies to educate and

12   communicate with consumers the benefits of

13   profiling and that these benefits outweigh the

14   risks, which also means that the people that hold

15   these databases have to make sure that they have

16   very good privacy policies in place and that they

17   enforce them.

18   MS. RICH: Next we have Evan Hendricks.

19   Evan is the Editor and Publisher of Privacy Times,

20   a biweekly newsletter that reports on privacy and

21   freedom of information law. He's also the author

22   of several other publications on consumer privacy,

23   including his book "Your Right to Privacy" and he's

24   Chairman of the U.S. Privacy Council.

25   He regularly lectures on information policy

181

1   issues in the U.S., Canada and Europe.

2   MR. HENDRICKS: Thank you, and thank you to

3   the FTC for the hard work they've put into this and

4   the opportunity.

5   In January I had the good fortune of

6   hearing Commissioner Swindle speak not once but

7   twice in different gatherings, and he said

8   something that I strongly agree with.

9   He said that when we talk about this issue,

10   we should not talk about it emotionally because it

11   can be an emotional issue, and it doesn't really

12   help. This is something we need really more light

13   than heat, so I made a commitment to him that when

14   I come before the FTC, I will not discuss this

15   emotionally.

16   And then I started thinking about it this

17   morning, and I started getting really mad because I

18   love to talk about this emotionally, but I'm a man

19   of my word, so I can't do that.

20   Seriously I think that we should speak

21   about this in cool and analytical ways, and I

22   think, first of all, there's a greater irony here,

23   and one of the ironies is that the direct marketing

24   industry was subsidized by the taxpayers. The

25   direct marketing industry was able to get public

182

 1   records at low or no cost, which was a great way to

 2   start a business if you can get your primary source

 3   that makes your business possible paid for by

 4   taxpayers.

 5   We've seen it -- and that's not such a bad

 6   thing. We've seen it with investment in computer

 7   chips by the Defense Department has led to the

 8   computer revolution, but let's recognize that as

 9   people speak against government regulation, what

10   got them to a point where they can speak about

11   that.

12   Second of all, I think already from today

13   and all the years I've seen leading up to this, on

14   the issue of warranty cards, I think there's enough

15   evidence to justify an investigation of unfair and

16   deceptive trade practices.

17   I think it's widely understood that

18   consumers fill out warranty cards thinking that

19   they need to do this for the warranty to be good,

20   and in fact you do not need to fill out a warranty

21   card for the warranty to be good.

22   The purpose of warranty cards is generally

23   to collect information by database companies. It

24   is then sold and used for other purposes, and

25   warranty cards are one of the primary sources of

183

1   unlisted phone numbers, which people are unable --

2   companies are unable to buy from phone companies,

3   but they can get them.

4   And I think it shows that people who pay

5   extra for an unlisted phone number would not be

6   giving their unlisted phone numbers if they knew

7   that information was going to be sold on the open

8   market, so I think we have a real problem there

9   that deserves official attention.

10   I think another example -- since I only

11   have three minutes, another example of something

12   that cries out for concern is say a company like

13   American Student Lists based in New York.

14   Factually, for instance, they have over 12 million

15   names of children ranging in age from 2 to 13 years

16   representing PK through 8th grade. All names are

17   selectable by age, birth date and heads of

18   households, and approximately 25 million age birth

19   through 17 compiled from numerous direct response

20   sources selectable by age, birth date, head of

21   household, income and geography.

22   Well, I doubt that most of the people in

23   those categories or their parents really had a

24   chance to exercise much in the way of notice and

25   choice.

184

1   A third area of I think concern which now

2   -- finally the good thing about the workshop -- is

3   it is being described as a very routine process and

4   it has been for years, but that is not known to

5   consumers, is the idea of enhancing your database,

6   which really means by virtue of being a customer of

7   a bank or of an Internet provider or whatever,

8   because you're a customer, then they go to outside

9   sources of data and fatten their file on you

10   saying, This is what kind of car you drive, this is

11   what kind of home you own, this is your estimated

12   income, do you have children.

13   And I think that there is again no notice,

14   awareness or education to consumers about what's

15   happening and certainly no rights for individuals

16   to do anything about it; and I think that is a very

17   significant privacy issue because if you join a

18   company, you know they're going to have information

19   on you as a customer, but when they merge

20   information, they're basically creating a whole new

21   file that you don't know about.

22   I think also the whole issue of public

23   records, I think that in public records, it's a

24   difficult issue. As a FOIA advocate, I think there

25   should be public access to public records, but when

185

1   it's personal data, I think we should apply the

2   purpose test that we find in Fair Information

3   Practices and that if it's a driving record, it can

4   be accessed for driving purposes.

5   Well, if it's a voter record, and in answer

6   to one of the earlier questions, Are there

7   restrictions on public records, half the states

8   have laws that say you cannot use voting records

9   and the other half don't, but I think the idea is

10   that if it will interfere with people's right to

11   vote, if they're concerned that their information

12   will be used for commercial purposes, that's the

13   purpose of the privacy law there.

14   I think we have to apply that kind of

15   purpose test where people can get access to a

16   voter's list if they're doing a campaign. How do

17   we do that? I think one way to do it is that I

18   think we should have to certify to the record

19   holder that you're using it for this purpose and

20   then have a notice sent to the data subject so they

21   know that someone has accessed their record.

22   That can be done either by postcard or

23   electronically to reduce cost, but I think that's

24   the direction we need to go to handle the public

25   records issue.

1   My final point is that I think there's a

2   lot of important players missing at this workshop

3   starting with Acxiom, which has records on over a

4   hundred million Americans, something like 120

5   million Americans pulled from all sorts of sources.

6   I commend you to two articles in the Washington

7   Post that dealt with Acxiom over the last couple

8   years.

9   I think a lot of hard work goes into

10   putting a workshop together like this all the way

11   up and down the Commission, and I think it's a

12   disservice to the Commission and the American

13   public if a major player like Acxiom and other

14   players like that don't participate to shed light

15   on what they do.

16   Thank you.

17   MS. RICH: Our next panelist is Rick Lane.

18   He's the director of E-Commerce and Internet

19   Technology for the U.S. Chamber of Commerce, where

20   he's responsible for coordinating the development

21   and implementation of the Chamber's E-commerce and

22   technology, legislative, and policy initiatives.

23   Mr. Lane has served in leadership positions

24   on a variety of federal, state and local

25   commissions and committees, including the

1   Montgomery County Cable and Communications Advisory

2   Committee.

3   Rick?

4   MR. LANE: Thank you very much.   I just

5   have a quick question.   How many people in the

6   audience have started a small business, have

7   started their own business?

8   That's what this is all about.   That's what

9   we're talking about in the free flow of information

10   and being able to have entrepreneurialism in this

11   country.

12   I started my own business called Cyber

13   Sports.   We spent a lot of money in development of

14   a product, and basically what the product was was a

15   database that college and university sports

16   programs could use to help track the college

17   recruits that they were recruiting through the

18   recruiting process.

19   In the old days they had paper files, and

20   they had problems complying with NCAA requirements,

21   but how did I get that product to market?   It was

22   easy for the most part to develop the product, but

23   how did we target our audience?   Our audience was

24   college coaches.

25   What we did was, first, we looked and

1   thought, Well, we can call every college and

2   university sports program in the country. I think

3   there are about 5,000 colleges. We were four

4   people. We couldn't afford to do that.

5   So what we did was we found a list that was

6   already available, that had information on all the

7   college coaches in every sport across the country.

8   It made our life easier. Then we got additional

9   information from other sources that put on top of

10   it the coaches win-loss records.

11   So we saw those coaches that were losing

12   would be a better potential market for our product

13   than those that were winning because the ones who

14   were winning figured, Hey, we already understand

15   this game.

16   And then on top of that, we took the

17   information of size of school because what we found

18   was the smaller the school, the more kids that they

19   had to recruit because they didn't have name

20   recognition.

21   I have a nephew who is six-three, 215, the

22   fastest kid on the team. He's not hard to find.

23   He's going to be recruited by Michigan and Ohio

24   State and other schools are going to find him and

25   probably offer him a scholarship, but what about

189

1   the kids who are in the smaller towns and how do we

2   get information about them?

3   Here's the next part of the process, which

4   is people send information on college kids

5   throughout the country into these coaches'

6   databases which they search on grade point

7   averages, height, weight, positions and they fill

8   them.

9   Now, what we're talking about is, Is that a

10   bad thing? Is offering kids scholarships a bad

11   endeavor? We have information, these college

12   coaches, on thousands of kids based on public

13   information through newspaper articles and so on

14   and so forth.

15   Yet they are using it to offer kids

16   scholarships, and those of us who enjoy March

17   Madness think, well, maybe it's not a bad idea at

18   all, but what we found is the academic side of the

19   colleges liked it because we were tracking grades

20   and other information for the kids that were being

21   sent in, but then other departments who were

22   offering scholarships began using our software to

23   offer kids scholarships for music and academic

24   scholarships and drama and so on and so forth.

25   So the information flow is critical. We

1   looked at it in Acxiom, yes, big macro, large

2   company, important to look at, but there are also a

3   lot of smaller, targeted uses of information

4   database and flow that is beneficial to the

5   foundation of this economy and how we operate.

6   So from our standpoint, we look at this

7   issue from a small business perspective. Let's

8   give small businesses the opportunity to grow and

9   survive and to create competition in the markets

10   unlike in the EU, and let's not arbitrarily just

11   cut that information flow off.

12   Thank you.

13   MS. RICH: Greg Miller is Interim Chief

14   Privacy Officer and Vice President of Corporate

15   Development for MEconomy, an Internet privacy

16   infrastructure venture. Before joining that

17   company, Mr. Miller was Medicologic Netscape's

18   chief Internet strategist of governmental affairs

19   and a director of strategic marketing for Netscape.

20   Mr. Miller has worked on issues involving

21   technical Internet infrastructure, online marketing

22   strategy, including personalization and data

23   warehousing, and Internet security and privacy

24   policy issues.

25   Greg?

191

1   MR. MILLER: Thank you, and I want to thank

2   the Commission for inviting me to participate this

3   afternoon.

4   Actually a little bit beyond MEconomy, I

5   have the privilege of being a venture capitalist,

6   not to be confused with capitalist, so MEconomy is

7   one of my portfolio companies.

8   But in the process of doing that, I

9   facilitate the development of emerging security and

10   privacy companies in the digital economy and advise

11   up-starts on issues of consumer privacy and

12   information security, and two very different, yet

13   perhaps paradoxically complementary sectors of

14   digital entertainment and U.S. health care.

15   I've been asked here today to participate

16   with my esteemed colleagues on an exploratory

17   discussion on the effects to business and consumers

18   of the merger and exchange of consumer information

19   and digital economy.

20   And of potential applicability to this

21   discussion, I spent the last six months working

22   with a client start-up to engineer an inflow

23   mediation and user registration system that was

24   designed specifically to address required

25   consorting of offline and online consumer

 1   information for multiple sources in order to create

 2   the best possible user experience and online

 3   digital entertainment while simultaneously

 4   respecting the privacy of those subscribers.

 5   Our solution, which we dubbed JOIN for

 6   "just opt-in," addressed many of the issues raised

 7   by this workshop, so the net of my work there, as

 8   it may contribute to today's discourse, can

 9   probably be summed up as follows: Over time the

10   convergence, Consortium and brokering of personally

11   identifiable information, or PII, we believe will

12   require a balancing test between the needs of

13   business and the needs of consumers, nothing too

14   profound there.

15   And I can see the broken smiles of the

16   lawyers among us. I call it YABT, "yet another

17   balancing test," and thankfully for all of us I'm

18   going to avoid going down that particular rat hole

19   of jurisprudence.

20   But anyway, what we learned last year in

21   this online music start-up was that consumers might

22   not worry about privacy per se as much as they

23   worry about surprises and uninvited interruptions,

24   and apparently Seth Goddin this week concurs at

25   least in part with that finding in the current

193

1   issue of Red Herring Magazine.

2   So I submit that consumers simply want to

3   be left alone and are not interested in being

4   interrupted, unless they've agreed to such as part

5   of the deal for receiving the information, product

6   or service that they're seeking.

7   I also submit that the majority of

8   businesses are not interested in snooping but

9   simply selling more products and services. For

10   business success in the digital economy means

11   gathering information to improve the customer

12   experience and relationship.

13   Compiling information on consumers from

14   whatever source is legally available should be

15   intended to improve the customer experience and

16   nothing more, and this may mean not only sharing

17   and consorting of PII, but synthesis of data into

18   homogenized databases.

19   This can raise potential concerns. The

20   ease with which PII can be extrapolated is

21   improving -- it's proving really possible to be a

22   very powerful thing and perhaps to one's detriment.

23   Witness Web M.D.'s move last week or the

24   week before to rescind their contractual

25   obligations to provide certain data to Quintiles,

194

1   one of their supply chain trading partners, due to

2   the technical wherewithal to ascertain an identity

3   with only a date of birth and a postal code.

4   I submit there are demonstrative benefits

5   to PII compilation and the downside in terms of

6   consumers' lack of confidence in business to do the

7   right thing or unwillingness to participate I think

8   can be addressed through what we call permission

9   based approaches to the data gathering use. Of

10   course, consumers should be aware of the possible

11   misuse of PII but also understand the cost benefit.

12   So through that work we also came to the

13   conclusion that unless and until the incentives of

14   business and consumers are matched in a manner that

15   encourages and authorizes the compilation and usage

16   of PII, something we're studying right now at

17   MEconomy, this so-called digital economy we think

18   may stall.

19   For the consumer the concern should

20   probably run to security more than privacy as the

21   real threat may lie in identity theft.

22   Unfortunately we weren't able to find a lot of

23   empirical evidence last year on the use or misuse

24   of PII.

25   I think the digital economy is still fairly

1   nascent, but I think prospectively industry should

2   focus on the now well settled principles of notice,

3   choice and access, and as they're equally important

4   in the compilation of PII, we think the consumer

5   should be notified of information gathering

6   practices and policies whenever they're used in any

7   service, online or not, and where appropriate or

8   practical given the choice to participate in

9   advance of such gathering.

10   We think the compiled PII by business

11   should be accessible to the consumer's review, too,

12   and we think applying these three principles with

13   equal force and meaningful standards for each

14   empowers the consumer to take an active role in

15   protecting their own identity and its uses.

16   So as we grapple with the complex issues of

17   the underlying and I think most valuable commodity

18   of a digital economy, PII, I believe that notice,

19   choice and access can serve as safeguards for over-

20   reaching data collection, and I think that that

21   would be the basis for my contributions today, if

22   any, that are hopefully useful.

23   Thank you.

24   MS. RICH: Thanks.   Lastly Brian Tretick is

25   a principal with Ernst & Young, who works in the

1   area of global privacy assurance and advisory

2   services. He serves clients in the online

3   financial services, retail and software industries

4   focusing on the technological, organizational,

5   regulatory and third-party relationship aspects of

6   data privacy.

7   He also works in the firm's global privacy

8   practice where he helps to provide various

9   consolidated services, technical, advisory, and

10   legal, to Ernst & Young's global clients. Brian?

11   MR. TRETICK: Thank you, Jessica. Prior to

12   this panel, you heard from marketers, and I

13   represent here the assurance industry.

14   I want to talk a little bit about what

15   companies are doing, especially companies that hold

16   on to marketing information, hold on to information

17   about their customers, merge third-party

18   information with that to get to know their

19   customers better and perhaps then provide an avenue

20   for other parties, their merchant partners,

21   business partners, to reach the company's customers

22   with those third-party messages.

23   First off, I would like to talk a little

24   bit about the organizational issues, namely, the

25   appointment of privacy officials, and these aren't

197

1   the privacy officials, the celebrity CPOs that were

2   appointed over the last year, year and a half.

3   These are people with a lot less glamor.

4   They have assurance, audit and compliance

5   responsibilities, so what we're doing, we're seeing

6   a push, an evolution of privacy and privacy

7   responsibilities out of the PR, the business

8   development type environments and down into the

9   business.

10   We're seeing an emergence of the roles and

11   responsibilities, the policies and procedures out

12   of marketing groups for marketing data, although

13   they need to keep executing those policies and

14   procedures. There's someone with authority and

15   accountability in companies who is much more,

16   pardon the expression, humorless about the use of

17   information because they're much more regimented

18   and disciplined in their backgrounds.

19   So we're seeing those again

20   accountabilities and authorities extending outside

21   of the marketing arrangement, marketing groups, and

22   into business development, into other compliance

23   and auditing functions.

24   We're seeing the extension of security and

25   controls, again not just on Web sites. All this

1   data is back in enterprise systems and increasing

2   technical, procedural controls in these situations,

3   and also assurances where management needs to

4   establish confidence among themselves that their

5   technology groups, that their business development

6   groups, customer service groups, marketing groups,

7   sort of fulfillment groups, are all meeting these

8   policies and procedures, these internal policies

9   and procedures.

10   So they're seeking assurance internally and

11   externally on these practices. They're providing

12   training and awareness for their employees and

13   third-party vendors on their policies, on their

14   detailed practices, dos and don'ts, what they

15   should and should not do regarding the use of

16   collected data.

17   And they're also reregulating their

18   dealings with third parties, with people who they

19   receive information from and people who they

20   provide information to, vetting them, selecting

21   them carefully and doing due diligence and

22   including specific terms of use in contracts with

23   third parties and also then various verification

24   and monitoring.

25   The final point here is that these

199

1   companies are working again internally or with

2   third parties to establish assurances that their

3   controls are in place to prevent bad things from

4   happening, to discourage bad things from happening,

5   and to put controls in place to encourage the right

6   things, the appropriate business practices to

7   happen.

8   Thank you.

9   MS. RICH: Thanks to everybody for your

10   prepared statements.

11   We thought it would be useful next to open

12   up the panel for a discussion of some of the issues

13   you touched on in your opening statements.   Some of

14   you have identified ways in which consumers and

15   businesses benefit from the merger and exchange of

16   data, for example, better targeting of ads, lower

17   costs, better customer service, lowering end

18   barriers for start-up, other examples.

19   I think it would be useful if the panelists

20   expanded on some of these points and had a chance

21   to comment on others' points that were made in this

22   area, and also if anybody has data to support or

23   even contradict the points they're making, if you

24   could mention it now, I think it would make for a

25   better discussion if there was any data and

200

1   everyone could hear about it.

2   I guess Jason is putting his tent up, so he

3   would like to start it off.

4   DR. CATLETT: Thanks very much. Let me

5   talk about dynamic pricing a little. There's very

6   little data on this because companies don't put out

7   press releases saying," We are able to gouge our

8   customers to the extent of $6 million."

9   However, I would point you to an article in

10   Harvard Business Review last month that says that

11   an unnamed consumer electronics store was able to

12   differentiate between price sensitive consumers and

13   price insensitive consumers who were in a hurry and

14   to charge the more hurried customers a 20 percent

15   premium over the more diligent shopper, so that's

16   the only empirical data point that I have about

17   dynamic pricing, an area that's shrouded in

18   secrecy.

19   What could we possibly do about dynamic

20   pricing? Well, there's a diversity of opinion

21   about whether this is a good thing. The airline

22   industry does differential pricing, not based on

23   personal information, but whether, for example, you

24   want to be home with your wife and children on

25   Saturday night.

1   A benefit to rationing that, and I think

2   there's a diversity of opinion on whether dynamic

3   pricing is a good thing.

4   What privacy protections are necessary in

5   that environment? I believe the appropriate one

6   here is that adopted in the EU's data directive

7   which gives the data subject not only the right to

8   see the base data on which the decisions are made,

9   but also to have an automated decision-making

10   process explained to him or her.

11   So that, for example, if an E-commerce

12   merchant is charging Fred $2 less for a paperback

13   book than it is charging me, then I can, in

14   principle, ask to have that decision-making process

15   explained to me, and then the merchant can say,

16   "Well, it's because of your past behavior in this

17   area," and then at least I have some understanding

18   on which to base my future behavior.

19   MS. RICH: Is that Rick down there?

20   MR. LANE: Yes. Just a couple points. On

21   the dynamic pricing issue, obviously that just puts

22   up red flags for us in terms of you're dictating

23   how businesses are going to charge particular

24   customers for particular items. Does it mean

25   dynamic pricing includes presenting certain

202

        1   customers with coupons that provide a 10 percent

        2   discount over maybe my neighbor who doesn't get

        3   that and based on my buying habits, and so that is

        4   obviously of concern.

        5   Also market forces, if what happened at

        6   Amazon.com is accurate and all this brew-ha-ha

        7   erupted, obviously there is concern in the

        8   marketplace that reacted very quickly and swiftly

        9   that consumers weren't ready for that or did not

       10   appreciate that, and it stops, so there are market

       11   forces already out there.

       12   Also the direct marketing that Jason put

       13   forth in his discussion about the increase in

       14   direct marketing over the course of time, well,

       15   yes, obviously there's been more mailings done.

       16   There are more people in the country.

       17   So, of course, you're going to have more

       18   mailings. There's more businesses. There's more

       19   small businesses, and we've had a dynamic growth

       20   over the past couple years. It's called economic

       21   growth. I thought it was a good thing.

       22   So, yes, you're going to have more direct

       23   marketing out there, but the fact is you're getting

       24   less mail that's not of interest to you, and that's

       25   a critical point, and that's what this is all

1   about.

2   DR. CATLETT: Could I respond to that

3   quickly? There are several factors at work, the

4   increase in population, the increase in the price

5   of paper and the price of postage, which Jerry I

6   guess constantly is working on, all work to cause

7   the total number of solicitations to vary for a

8   number of different areas.

9   But I think if you learn DM Math 101, you

10   will find that more information means more total

11   solicitations, more accepted solicitations, but

12   also more unwanted solicitations.

13   And on the issue of dynamic pricing, I

14   didn't seek to say that the Federal Trade

15   Commission should stop dynamic pricing or stop a

16   company from offering a coupon to a subset of its

17   customers based on the Claritas Prism rating or

18   whatever criterion.

19   I simply think that from the point of view

20   of privacy and fair information practices, the

21   consumer should have the right to see the

22   information that that decision is being based on.

23   The information may be incorrect, and they may be

24   missing out on something that they might otherwise

25   be entitled to, and the decision-making process

204

1   should be transparent.

2   If there is a trust gap, and I agree with

3   Commissioner Swindle and the many other speakers

4   who have said that there is a trust gap here, the

5   way to close that gap surely is greater

6   transparency, to give the consumer the right to see

7   what's going on and the right to delete it if they

8   don't want it.

9   MS. RICH: Evan, you've been waiting

10   patiently, calmly.

11   MR. HENDRICKS: And unemotionally too.

12   MR. RICH: Unemotionally, yes.

13   MR. HENDRICKS: Well, let's talk about

14   small business. If you look -- I commend everyone

15   to the latest study from Forrester. Jason cited

16   one earlier in our Privacy Times. It's out on the

17   table. We report on the latest Forrester which

18   looks at wireless, how privacy is not only integral

19   to wireless, but privacy is integral -- it's the

20   core business issue, and that it has to be dealt

21   with top to bottom or businesses will suffer.

22   And Forrester staff are not consumer

23   advocates or political. They're just worried about

24   their clients' bottom line, and I think it's a very

25   important analysis.

1   Let's talk about small business. I mean,

2   so much of being in business depends on your

3   judgment as a businessman and what is your business

4   model, and so sometimes you need information to

5   make your business go, and sometimes you can

6   configure your business so you don't need to rely

7   on people's personal data.

8   I started my small business in January

9   1981, and I had $3 in my pocket, and I've not

10   borrowed money, and I'm still in small business

11   and -- is the business you described still going?

12   MR. LANE: It's the number 1 recruiting

13   software in the country.

14   MR. HENDRICKS: Excellent, excellent. So

15   we like that, but I think the other thing that

16   happened to be in the 1980s is when the federal

17   agencies were making a lot of claims about computer

18   matching and that computer matching -- when I

19   wanted to match databases from different agencies

20   to fight fraud, they would make these projections

21   about how bad fraud was among federal agencies.

22   And I was part of studies that actually

23   drilled down and looked at the numbers, and we

24   found that the costs and the fraud projections were

25   completely specious. There was no basis in fact to

1   them, and that they were just pulling numbers out

2   of the air.

3   So I look in today's Wall Street Journal,

4   and I see that the cost of the 90 largest financial

5   institutions will be $17 billion for some sort of

6   restrictions on sharing or selling customer

7   information, and Fred is quoted as saying that the

8   costs run into the trillions, so I look forward to

9   looking at those numbers too.

10   I'm very skeptical that these will hold up

11   to objective analysis and that the one thing when

12   you hear about Gramm Leach Bliley, notices will be

13   going to customers by banks of information

14   practices and privacy policy.

15   But Gramm Leach Bliley, the provisions in

16   there were -- that's what the banking lobby wanted.

17   They got what they wanted in this bill, and the

18   other proposals advocated by the consumer advocacy

19   community were rejected.

20   So this is a case where maybe they didn't

21   think out long enough what really were the best

22   privacy standards and the most cost efficient ones.

23   MS. RICH: Fred?

24   MR. CATE: Thank you very much. I think

25   one of the points Evan makes, he raises one, and

1   frankly this goes to something Jason said which

2   might be worth following up on, several people have

3   mentioned, and Evan just did then, the question of

4   how many people don't engage in an activity because

5   of privacy fears and trying to put numbers, and

6   Forrester certainly tried to do that.

7   I think there's some reason to be a little

8   skeptical of that, and I think Europe is the reason

9   for that. Europe offers the most restrictive set

10   of privacy laws we have on the books.

11   The polling data on reasons for staying

12   offline is just as high as in the U.S., so in the

13   presence of very high legal protection, you have a

14   very high anxiety rate.

15   Moreover, something else we seem to know is

16   that there's a certain disconnect here between what

17   you want to be worried about and what you are

18   worried about, that what we might perceive because

19   we don't know, because we don't understand, and

20   that this is also reflected frankly in a lot of

21   these -- a lot of these numbers.

22   And if you read the whole survey you see

23   what they were really talking about was something

24   different. They were talking about security or

25   they were talking about some specific issue, not

208

1   the question of, Is this information going to be

2   shared.

3   They're worried about, Is the information

4   even going to get to the end point, but this

5   reminds me -- this is my segue alert. This reminds

6   me of Jason's point, which I think actually is

7   excellent, dynamic pricing is an issue. If it's a

8   problem, it's a problem that should be looked at as

9   a phenomenon itself.

10   And if Commissioner Swindle can get me a

11   cheaper fare home because I'm not going to be

12   subject to the sort of pricing that the airlines

13   use, I think that would be terrific.

14   Unfortunately, I guess jurisdiction doesn't extend

15   there.

16   But it highlights the sort of need to focus

17   on what is the use of the information that causes

18   the problem; in other words, not what's the specter

19   of uncertainty. What's the way in which you can

20   sort of look across sort of all possible uses of

21   information.

22   But if in fact there is a use of

23   information, for example, we have all sorts of laws

24   in this country prohibiting discrimination, that

25   you would use information to discriminate in. We

 1   don't have nearly as many laws restricting the flow

 2   of that information. We have laws restricting the

 3   use of that information.

 4   You cannot use it to discriminate in

 5   certain ways, housing, public accommodations and so

 6   forth, and so I think really both of these points

 7   highlight the importance of focusing on

 8   demonstrated behavior and real harms as opposed to

 9   sort of speculation and system wide regulation of

10   information flows.

11   MS. RICH: Mary?

12   MS. CULNAN: This is another segue alert,

13   but I think for the business people in the

14   audience, I mean, one way to think about privacy,

15   it's not really privacy, it's really disclosure.

16   You want consumers to be comfortable disclosing

17   information and allowing it to be used for

18   marketing.

19   And there have been a couple of good Harris

20   surveys that have looked at people's willingness to

21   disclose. There was one done in 1997 so these were

22   mostly computer geeks in the sample because at that

23   time everybody wasn't on AOL like they are now.

24   But they asked some questions about, Have

25   you ever either lied or not disclosed information

210

1   to a Web site when they asked for it, and everybody

2   knows the numbers. A huge number of people say,

3   Yes, at some point I did do this.

4   So then they asked, Well, what if the Web

5   site told you, gave you notice and choice, and a

6   huge -- about half the people who did not disclose

7   before or lied say, "Yeah, I'll disclose my

8   information then," or if you already had a previous

9   relationship with a firm, then a lot of people

10   would disclose.

11   I think what it says is you've got to get

12   at least notice and choice into the equation, and

13   it does make people more comfortable.

14   Now, the other interesting side to this is

15   there is still a clump of people that under any

16   circumstances are still not comfortable disclosing,

17   and the issue is, What is it that would make these

18   people disclose or, in fact, is this just how

19   marketing works, and there's a segment of people

20   that don't want to do business online.

21   MS. RICH: Jason?

22   DR. CATLETT: Let me go from those

23   habitual, non responders, who comprise

24   approximately half of the United States, back to

25   the dynamic pricing issue.

211

1   Rick said that market forces have corrected

2   that, and in the case of Amazon, I would feel a lot

3   more comfortable if Amazon disclosed the fact that

4   they were doing dynamic pricing. This was not the

5   case. It was discovered by someone who talked

6   about it on an Internet discussion group, and then

7   it went out to the media.

8   So I think again the problem we have is a

9   lack of transparency here. If we want to

10   investigate the practice, we have a very difficult

11   time doing so, if we don't have a right of

12   consumers to see what information is being held

13   about them and how it is specifically being used in

14   their case.

15   MS. RICH: Since we seem to be moving

16   partly into what effect this has on consumers, let

17   me just go back to a point made earlier, which is

18   if there are cost efficiencies and lower costs

19   generally from being able to share data, are any of

20   these cost efficiencies passed on to consumers?

21   Has anyone measured that or thought about that?

22   No.

23   Another point I just wanted to go back to

24   before we move into effects on consumers completely

25   is I heard different statements being made about

212

1   whether the number of solicitations is really

2   reduced when you can share data and target more

3   efficiently with some people saying that, Yes,

4   people will get fewer solicitations and others

5   saying, Well, they'll be targeted more.

6   Does anyone have any data on that or any

7   information that would be useful in talking about

8   that issue?

9   Evan?

10   MR. HENDRICKS: Well, in the credit cards,

11   we do have data out, just in the last few months,

12   showing that the response rate for pre approved

13   credit card is plummeting, and I think that deals

14   -- I mean, here's a situation where they're able to

15   use credit bureau data, highly targeted, and it's

16   just a question of the market is so saturated, and

17   there's not much differentiation anymore among the

18   credit card offers.

19   So I can't remember, someone told me it was

20   .4 percent or something was the response rate, so

21   the customer acquisition is going much higher, and

22   that's many factors.

23   DR. CATLETT: They key point there is the

24   number of credit card solicitations is going up.

25   MS. RICH: Jerry?

213

1   MR. CERASALE: The basic -- this isn't

2   precise data, but the basic use of mail

3   solicitation tends to be standard mail, although

4   there are solicitations that go out first class,

5   and standard mail growth is growing faster than the

6   rest of the mail volume is growing, but

7   significantly below what would be expected in

8   the -- what was expected in the growing economy.

9   The Postal Service is coming in and asking

10   for new rates and so forth based on new market

11   forces, so that the amount of total volume of

12   standard mail is not growing, what would be

13   expected in the economy.

14   One of the things you can see has changed

15   over time, however, is what used to be known as

16   resident or occupant mail, that in standard mail

17   the non resident, non occupant mail percentage of

18   standard mail is growing, meaning that the

19   targeting has increased. It's not just the

20   saturation shock on hitting every house everywhere,

21   even though those have the lowest postage rates

22   offered by the Postal Service.

23   So that type of data we have seen as well,

24   and the solicitations also tend to follow a pattern

25   of the economy, that if the economy turns down, you

1   tend to get a significant increase in standard mail

2   solicitations to try to drum up the business that's

3   being lost, and that lags the drop in the economy

4   about six months to nine months before that

5   plummets down as it follows the economy.

6   So that's what's happening. You have an

7   increase in targeted pieces, less saturation pieces

8   going through the mail, but they are growing less

9   rapidly than they have historically based upon

10   what's happening in the economy.

11   DR. CATLETT: Jerry, could you just clarify

12   that standard mail is what used to be called third

13   class mail?

14   MR. CERASALE: Yes, that's what the Postal

15   Service used to call third class mail. They now

16   changed it to standard.

17   MS. RICH: Before we get too deep into

18   consumers, I realize I left out the piece of -- we

19   talked about the benefits for businesses of these

20   practices.

21   Does Greg or Brian or anyone else want to

22   talk about some of the downsides or the risks for

23   businesses of these practices?

24   MR. MILLER: We both probably have

25   interesting remarks to make about this, and just

1   perhaps as a segue from the business side over to

2   the consumer side, I want to speak to you a moment

3   about infrastructure cost on the business side and

4   then how that transitions over to consumers.

5   And I have two quick case points for you

6   that would be great for you to comment on too, and

7   I will start with health care, which is where I

8   spent a lot of time in the medical records space,

9   and what we were trying to do at Medicalogic was

10   give to the consumer for the first time in history

11   a secure, authorized access to their authentic

12   medical history.

13   Well, it turns out that for most of us, our

14   medical history is comprised of several records,

15   our primary care physician and at least a couple of

16   specialists, and so what we were trying to do was

17   give a view port to that comprehensive medical

18   history, and that required literally the opt-in of

19   several physicians and the proactive relationship

20   building that went on with the patient to encourage

21   them to allow that.

22   That required a lot of infrastructure cost

23   for us in the consorting and homogenizing of that

24   data and creating the necessary safeguards to even

25   create Chinese walls, if you will, between the

1   dermatologist and the OB-GYN and the primary care

2   physician, so there was a view port challenge

3   there.

4   In the entertainment space, the most recent

5   case, we had a very challenging one with -- another

6   one of our panelists, Ted Wham and I worked

7   together on a project in the music space, and the

8   problem we had there was when you go buy music, you

9   don't say to yourself, I've got to go get me one of

10   those Sony records. You say, I want to go buy a

11   Dave Matthews album.

12   You, the consumer, purchase by artist, but

13   the music industry, by which I mean the five record

14   labels that control 90 percent of the music that's

15   distributed worldwide, have their view of the world

16   on you.

17   So we literally had to engineer what we

18   called a data escrow service to ensure that privacy

19   policies across five labels actually reconciled

20   with one another and then the JOIN, the just opt-in

21   program, was the means by which we encouraged the

22   consumer to get the experience that we're really

23   looking for which was a unified locker service

24   which allowed them to compile all music they've

25   ever purchased across any label from any retailer

217

1   in history into one homogenized database.

2   This really presented a lot of problems

3   because all the labels jumped up immediately and

4   said, Not on my watch are you going to be mixing my

5   data with the data of Universal without my customer

6   explicit opting in says BMG, so we literally had to

7   create this membrane.

8   This produced some substantial costs, and I

9   dare say it may have been the straw that broke the

10   camel's back because unfortunately that company is

11   now in receivership. They spent tons of money on

12   infrastructure to build the data escrow service

13   that would ensure the privacy policies of five

14   labels were maintained and protected and then still

15   get the subscriber, the consumer, opting in to

16   participate.

17   And I think that put a lot of pressure on

18   them from the standpoint of ensuring privacy as

19   well as building infrastructure that would support

20   and then shield them from a certain amount of

21   liability which I think segues over to you.

22   MR. HENDRICKS: Also, Greg, wouldn't an FTC

23   standard, a uniform standard solve that problem

24   across those five Web sites?

25   MR. MILLER: I think to a certain extent

218

1   that's possible, yeah, but it's interesting the

2   challenge of being a lawyer, working with lawyers

3   and their view of each of their privacy policies.

4   MR. TRETICK: I think there are always some

5   risks in the exchange of any valuable asset, both

6   upstream and downstream from a marketing data

7   provider to a marketing data consumer company.

8   The providers are looking to make sure that

9   the information that they provide is going to

10   reputable and responsible parties and going to be

11   used in reputable and responsible manners, that

12   children's information that is being offered up

13   about all these school kids and college kids isn't

14   going out to market them, drugs, liquor, cigarettes

15   to athletes, things like that upstream.

16   Downstream is the same thing. We want to

17   make sure that when we receive information it's

18   coming from sources that got this data under again

19   a reputable and responsible regime and that we can

20   reach out and touch these customers and make sure

21   then that they're not annoyed by our message, that

22   the frequency of being able to be touched is

23   reasonable, that the method of touching these

24   customers is reasonable and responsible and

25   appropriate for that.

219

1   So these are the risks that are faced both

2   upstream and downstream.

3   MR. CERASALE: I think we're switching to

4   some risk to businesses. I think the first risk a

5   business has is they promise more than they can

6   deliver, so that you have to make sure that you

7   promise to do certain things and that you can and

8   will be able to do it.

9   The risk -- the real risk you have, a

10   business has in sharing information is to become

11   complacent and sloppy. If you don't treat the

12   information that's given to you as part of a trust

13   relationship, ensure that you have safeguards to

14   keep the data secure, you want to make sure -- as

15   you just said, you want to make sure to whom data

16   is being shared, what type of procedures, what type

17   of marketing piece is going out.

18   If you're just sharing data from one

19   marketer to another, you want to see what the

20   marketing piece is. You want to make sure if

21   you're -- for a one time use that the list is

22   seeded so you can see, to make sure the person you

23   dealt with actually does, in fact, live up to his,

24   her, its agreement they had with you.

25   So that those -- and you have to train your

1   employees as they work with -- we've seen that way

2   back with -- an example that was publicly stated

3   here with Metro Mail where on the 13th phone call,

4   an untrained person gave information out. You have

5   to make sure that you work that way because you can

6   quickly lose consumer trust.

7   A 60 Minutes program, something like that,

8   can destroy your business, so I think that that's a

9   big downside for businesses.

10   The upside is that you can try and grow and

11   expand and give people who don't have as many

12   choices more choices and so forth, but you can, if

13   you are reckless, totally destroy your business

14   with some mistakes.

15   MS. RICH: I'll take Jason, and we'll move

16   on.

17   DR. CATLETT: Thanks. Building on Jerry's

18   point there, it's not any danger to the individual

19   company. It's a danger to the collective trust by

20   consumers of companies and the technologies.

21   I would refer you to another Harvard

22   Business Review article by Susan Fornia called

23   "Preventing the Premature Death of Relationship

24   Marketing" in which she tells -- gives an example

25   of a supermarket with a loyalty card that would

221

1   send out personalized letters saying, You haven't

2   bought X lately, why don't you come in and buy some

3   more.

4   And of course, inevitably some woman became

5   pregnant, and the company -- the supermarket sent

6   out a solicitation saying, Why don't you come in

7   and buy some more tampons.

8   There are a number of similar horror

9   stories. We heard the miscarriage example this

10   morning. We've heard the prison inmate sending the

11   personal letter to Beverly Dennis.

12   It's very difficult to quantify the degree

13   to which the average consumer is aware of these

14   horror stories, but I think that the American

15   public is largely aware that they have very few

16   rights in these cases. The company takes a PR hit.

17   They change supplier, but what about the individual

18   whose data was used inappropriately?

19   And I submit that the American consumer,

20   under current law in the U.S., has inadequate

21   recourse.

22   MS. RICH: Well, in addition to these

23   issues Jason has just raised about how consumers

24   are affected, I think the main concern for

25   consumers that I heard identified in the opening

222

1   statements was whether the practices are

2   transparent to consumers.

3   Mary, you're nodding. Would you like to

4   expand on the points you raised earlier in the

5   panel?

6   MS. CULNAN: I just don't think people know

7   what's -- the average consumer knows what's going

8   on, and then the problem is, and it exacerbates the

9   trust gap, that people are surprised. Then they

10   become unhappy.

11   And it's when -- wasn't what they were

12   expecting, wasn't the bargain that they bought

13   into, and so then they write to their members in

14   Congress or they do whatever, there end up being

15   stories in the newspaper, et cetera, and it causes

16   a lot of problems for the collective business

17   community.

18   One of the things I forgot to mention

19   before too, the people who were sort of the least

20   trusting and the more concerned about privacy and

21   the least willing to disclose were also the ones

22   who were most likely to favor legislation, so I

23   think there's a take-away there.

24   I think the industry can do a lot to help

25   educate people as they've done in other areas,

223

1   online privacy, kids privacy. There were some

2   terrific presentations at today's sessions. Why

3   not put them up on the Web? Why not try to get

4   people to go there?

5   I think the DMA can play a big role in

6   terms of trying to push your members along to do

7   better disclosures by putting -- changing the model

8   disclosures in the compliance manuals to be more

9   forthcoming about what is really happening to your

10   information when it's shared or when you provide

11   it. I think -- go ahead.

12   MS. RICH: Before we talk about this issue,

13   could somebody, Jerry, Brian, somebody describe

14   what kind of notice is being provided regarding

15   these practices?

16   MR. CERASALE: I can start this at least.

17   Notice has been provided by catalogers, for

18   example, for an awful long time, and the notices

19   generally -- I have a box of catalogs I was going

20   to give Martha, I forgot to do it, I'll do it later

21   now, that show on the order forms, basically is

22   where they are, mailing, preference service

23   information, so forth on how to, and they state

24   basically that information is shared with third

25   parties to send you -- to market to you offers that

1   you might be interested in, and if you don't want

2   that, either call this number or write to us here.

3   MS. RICH: Does that encompass --

4   MR. CERASALE: That's the notice that

5   generally comes in the off -- I would say in the

6   offline world.

7   Online is a little different in the sense

8   that there's more space. The real estate is fairly

9   inexpensive, and some privacy policies are very

10   lengthy, as some people have heard when they went

11   to testify up on the Hill, a little bit too long,

12   so they can -- some of them are a little bit more

13   detailed in the offline world.

14   Plus if you have a network advertiser on

15   there, you have to add -- there's a whole slough of

16   more notices that are required.

17   MS. RICH: When you say the notice says we

18   share with third-party, does that include sharing

19   with compilers?

20   MR. CERASALE: Yes, that's the way it is

21   today, sharing with third parties for marketing

22   purposes to send you offers, and it does say for

23   marketing purposes, and that's where DMA requires

24   it be for marketing purposes as well, but that

25   would include that at this point, yes.

225

```
 1              MS. RICH:  Do the notices talk about

 2      bringing in data from third-party sources and to

 3      provide overlays or other enhancements?

 4              MR. CERASALE:  Generally the examples I

 5      have with catalogers, they do not.

 6              MS. CULNAN:  I would say, first of all, I

 7      think again saying you share for marketing

 8      purposes, most consumers understand that if you buy

 9      X, you get Y where Y is the same industry as X, but

10      they don't understand compilers.

11              Second thing -- and now I've forgotten what

12      I was going to say.

13              MS. RICH:  We'll come back to you.

14              MS. CULNAN:  Oh, oh, oh.  The enhancement

15      thing, I have seen -- there was one excellent

16      financial services notice about enhancement that

17      basically said, We do profiling, we do data mining,

18      we acquire third-party data, non credit report

19      data, to understand how you use our card and we use

20      this to serve you better, and they had an opt-out

21      form right with the notice, and you could mail that

22      back or call the 800 number.

23              Unfortunately, with the Gramm Leach Bliley

24      requirement, that doesn't cause companies to have

25      to specify how they're going to use information,
```

226

1   just what they collect and who they disclose it to.

2   That very nice statement disappeared from the Gramm

3   Leach Bliley notice that this company has sent out,

4   which is now their de facto privacy notice.

5   So I think that's an issue that's probably

6   not going to get Congress to act on it, but again

7   more disclosure I think makes people more

8   comfortable.

9   MS. RICH: Fred, were you going to address

10   this point?

11   MR. CATE: Yes, and I have to say I am

12   genuinely confused, and that is we talk a lot about

13   transparency and that we all want transparency and

14   we want more transparency, we want more disclosure.

15   On the other hand, we know as a statistical

16   matter people don't read these, and therefore we're

17   saying we're going to make ourselves feel better

18   about privacy because we're going to mail a lot

19   more notices to people so they can throw those

20   away, but we can then say we've met disclosure

21   obligations.

22   And what I wonder is if there isn't a

23   better way, in other words, if there isn't a way to

24   make -- to go back to that point.

25   I mean, two things that have been said.

 1   One is people don't want to be bothered, period. I

 2   think you could just stop there. It doesn't need

 3   to be qualified. They don't want to be bothered

 4   with privacy notices any more than they want to be

 5   bothered with anything else.

 6   And if you want empirical evidence of that,

 7   just go home and set your own browser so it asks

 8   you every time you get a cookie and see how long

 9   you live under that system.

10   You just don't want to be bothered. I

11   mean, it's that simple. You will set the default

12   to accept all cookies or you will stop browsing on

13   the Internet.   I'm only describing 97 percent of

14   the population. I know there are three of you out

15   there who will be different.

16   So is there a better way to provide to get

17   rid of the surprises, if you will, yet recognizing

18   people really don't want to be sort of educated

19   generally about this? I mean, as a professional

20   educator, I know how hard it is to hold the

21   attention of anybody at any time, but the idea of

22   providing sort of a lesson on privacy at point of

23   sale, it's a little easier maybe on the Internet.

24   But it also comes back to that problem of

25   thinking specifically about when are we talking in

228

1   a transaction and what is the impact on the

2   consumer depending upon when that is?

3   At time of collection it's probably much

4   easier, Why am I asking you for this information,

5   here's why I'm asking, but that requires of course

6   that we're only talking someone who is dealing

7   directly with the consumer. We're not talking

8   about any third-party activity there, and we're

9   talking about they're going to anticipate all

10   possible uses at that moment.

11   And of course remember that notice, if it's

12   complete, will be criticized as being overly

13   detailed, and if it is incomplete will be

14   criticized as forming a contract that doesn't

15   include all of its correct terms.

16   But what I worry about is the later use.

17   Back to the AOL example, AOL decides it wants to

18   start mailing disks to people's houses. It didn't

19   have any dealings with any of those people. It had

20   no chance to talk about consent with any of them.

21   It can't mail them notices for consent because to

22   do that, it would have to use the very information

23   we want them to get consent before they use.

24   What are they to do, buy ads educating

25   people, I'm a start-up business. You have $3 in

1   your pocket but you can buy an ad in the New York

2   Times saying, let me educate you about something we

3   know the public is not interested in generally

4   being educated about?

5   I think it's a real conundrum that frankly

6   none of us, and I'm certainly including me, have

7   done a very good job getting at.

8   MS. RICH: Evan?

9   MR. HENDRICKS: That's why I brought up

10   earlier, I think it has to be case by case. I

11   think we have to be practical here because nobody I

12   know in the privacy advocacy community wants to see

13   bad things done in the name of privacy.

14   That's why I brought up with the magazine

15   publishers, How about putting a box at the bottom

16   of the card? It's not going to cost you anything.

17   A lot of people -- and it's opt-out, which is the

18   altar that many people here are praying at, and

19   still there was no willingness to commit to

20   anything like that, and I think that evidence is a

21   certain level of bad faith, to be frank.

22   I think the one -- the other thing I fear

23   is like the two real harms to privacy, the most

24   extreme harms are identity theft which is supposed

25   to be the fastest growing crime in the U.S., and

1   information brokers, the guys that get your

2   information.

3   And for many years the credit reporting

4   agencies have been the easiest target for those

5   people, and I think because of litigation under the

6   Fair Credit Reporting Act and business cases and

7   settlements and losses, the credit reporting

8   agencies, you're going to see them tightening and

9   tightening and tightening the procedures and

10   protections against those two threats.

11   And what you're going to see is the

12   identity thieves are going to be turning to these

13   other sources of data, and so when the marketing

14   material says this will only be used for marketing

15   purposes, I think there's a real warning cloud out

16   there about these existing threats that you can

17   anticipate.

18   And finally, I have to point to the

19   ToySmart case which the FTC is familiar with. I

20   mean, here's a company that had a privacy policy.

21   It went bankrupt, and its privacy policy lost out

22   to its fiduciary duty to in that case the trustees

23   and the bankruptcy, that they had to sell their

24   data.

25   And I think that if a marketing company

1   basically says they only want to sell this

2   information for marketing, but if certain revenue

3   streams and opportunities come up which says that,

4   Well, you can sell more individual profiles for

5   different purposes for screening, then that's going

6   to create the same quandary because that

7   corporation will have a fiduciary duty to its

8   shareholders to go after those revenue streams.

9   MS. RICH: We'll take Greg and then Jason,

10   and then we'll open it up for questions.

11   MR. MILLER: Just a quick couple of points.

12   One, I also was sort of surprised this morning

13   about the response with regard to the check box on

14   the bottom of the card.

15   For some empirical data from the

16   entertainment industry from the focus groups we've

17   been working on, we actually got quite a different

18   result. We discovered that if we engage consumers,

19   a trust relationship was built.

20   We started to minimize the notion of

21   surprising, and we actually found there was an

22   updraft or an uptake in people opting in if you

23   gave them the permission to opt-in.

24   I think one of the big fears about this,

25   from the marketers is that, Gosh, if we start

232

1   asking people for permission, they're going to say

2   no.   That was a suggestion this morning that was

3   made that, no, people won't fill it out.   They'll

4   actually not opt-in.   In fact, we find -- we have

5   empirical data that shows they will.

6   Another point we found out is nobody reads

7   the privacy policies, as Professor Cate observed

8   correctly, and we once we started describing to

9   people the notions of data gathering and what can

10   be done with it, that was really what started

11   sending people into a tizzy because, let's face it,

12   people have no idea what an aggregator is.

13   They don't know the difference between an

14   aggregator and a marketer.   They couldn't recite

15   that slide up there to make a conscious decision

16   about whether they should participate or not, and

17   as you begin to educate them, you end up drifting

18   into this rat hole of technicalities and nuances.

19   So we had that problem, and to speak to Mr.

20   Cate's notion of what do we about it, one thing

21   that we have been experimenting with is the sort of

22   interactive privacy policy, and it was because on

23   advice of legal counsel, somebody started saying,

24   Guess what, it turns out it's not really a policy,

25   it runs more like an agreement, like a terms of

233

1   service agreement. We're going to find that a

2   privacy policy is in fact a contract, and that sent

3   up the red flag.

4   And we said, Okay, so we need to reengineer

5   the privacy policy and be an interactive document,

6   so what we did with the JOIN program is that we

7   asked people to actually read through the policy,

8   meanwhile in the back while we're consorting their

9   data and setting up their locker, and we asked them

10   to click off a check box between each major section

11   in the privacy policy.

12   And we started compiling that data to see

13   which sections people were reading and what they're

14   doing with it. It also gave us some affirmation

15   that they had at least seen the privacy policy,

16   whether they were going to do anything about it or

17   not, and we found that that was pretty instructive.

18   And then finally the last thing was that in

19   the focus groups that we ran, and they were in New

20   York and Texas and North Carolina and Seattle,

21   Washington, Los Angeles as I recall, it turned out

22   that the most common thing that people reacted to

23   about what would happen with their data was again

24   being surprised, being bothered, not being left

25   alone.

1   They didn't give permission to get that

2   piece of mail or that announcement or whatever, and

3   the second thing, identity theft. The second most

4   popular concern turned out to be identity theft,

5   and this is data, talking to people who are

6   consumers of musical and video entertainment and

7   are looking for ways to get that through the

8   Internet.

9   MS. RICH: Jason?

10   DR. CATLETT: Thanks. I think the solution

11   to Fred's conundrum about transparency is to

12   guarantee each individual access to the data about

13   them. If you think transparency means putting up a

14   long notice, I think that's very much mistaken.

15   Let's take the analogy with the federal

16   government departments. I don't read the mission

17   statement of every federal government department

18   that might have personal data about me, but I know

19   that if I think they're doing something wrong, I

20   can put in a FOIA request, find out the specific

21   data they have and see if I need to fix something

22   there.

23   So I think a similar principle of

24   transparency would provide a lot of assurances

25   about direct marketing companies. Unfortunately,

1   and other trade groups and companies have refused

2   not only to give general access to marketing data,

3   but also even at this workshop to show us specific

4   examples of known individuals who have consented to

5   it.

6   I think that's astonishingly arrogant, and

7   that the FTC should have a forceful response to

8   open up that transparency to the degree people

9   want.

10   MS. RICH: Let me follow up. Jerry, when

11   you said that the privacy policies, when they in

12   general talk about sharing with third-parties and

13   that encompasses sharing with compilers, is that --

14   some of the comments here made me realize we may

15   not have -- I didn't understand your response.

16   Does it actually discuss sharing with

17   compilers?

18   MR. CERASALE: No, no. It's sharing with

19   third parties. The view of DMA is that data that

20   is shared should be subject to a notice and an

21   opportunity to say no, and that data can be shared

22   with third-parties for marketing purposes and

23   compilers.

24   And I think Win talked about making sure

25   the information they received had come from

236

```
 1    marketers that had given notice and opt-out, so

 2    that's where it's at.

 3            As far as the general common notice, there

 4    is no statement concerning compilers at this point.

 5            MS. RICH:  We'll go to questions, but if

 6    Fred and Evan could -- did you want to say

 7    something?

 8            MR. HENDRICKS:  Go to questions.

 9            MS. RICH:  Fred, did you have something

10    very quick to say.

11            MR. CATE:  I just wanted to say, there is

12    now a data set, which Jason has reminded me of, and

13    that is if we're going to talk about the federal

14    FOIA, there's excellent data under what access

15    under FOIA costs, about the litigation it generates

16    and about the amount agencies spend on it.

17            At some point in the late 90s the agencies

18    stopped collecting data because the process of

19    collecting that data was high, but certainly for

20    the preceding 20 years, there's excellent data

21    which would be easily available to the Commission

22    on what complying with an access regime costs.

23            MS. RICH:  I saw some questions in the

24    audience, lots of questions.  This gentleman right

25    here was holding his hand up earlier, right here
```

1   with the gray or the -- I can't see in the light.

2   MR. O'HARROW: I don't know if this is

3   going to work. I'll talk into it.

4   MS. RICH: Could you say your name?

5   MR. O'HARROW: Robert O'Harrow. I'm a

6   reporter at The Washington Post, and I have written

7   a little bit about this over the last couple years.

8   MS. RICH: I didn't know who he was when I

9   called on him.

10   MR. O'HARROW: That's okay, and excuse me,

11   and one thing I thought was very interesting, and

12   I've actually noticed it for several years is the

13   discussion oftentimes found its way back to the

14   question of whether or not the use of data

15   warehousing, data mining and so on increases or

16   reduces the mail that an individual receives at

17   home.

18   And then the discussion sort of surrounds

19   that for quite awhile, and I guess I wanted to sort

20   of raise a question of whether that's really the

21   issue. It seems to me that in some ways it used to

22   be the issue, but in many cases it might be a

23   canard that tends to distract us from the larger

24   issue at hand, which I think is profiling.

25   And so I wanted to sort of raise that as an

238

1   open ended question, of whether or not that's

2   something that's salient at this point.

3   Secondarily, there was an assertion up

4   there that people don't want to be educated, and I

5   think what I've found in interviewing many, many

6   people and industry folks, academics and so on is

7   that the reality is that people don't want to read

8   legalistic privacy policies that are written to

9   meet a very low threshold for privacy disclosure.

10   I find it very difficult, and I've read a

11 lot of them, and some of them I've actually

12 understood. In fact, I would have to say as gently

13 as possible that I don't think anything could be

14 further from the truth, and that at my paper, it's

15 one of the most widely read subjects that we've

16 written about and that people can't seem to get

17 enough of true, clear, explanation.

18   And oftentimes a clear explanation will

19 create a great deal of anxiety which, to loop back

20 to my original assertion about the direct marketing

21 and the mail and so on, the real issue, is the

22 question is, Do people want to feel like they're

23 being watched, and charted without their

24 permission?

25   Just some food for thought or if anybody

1   wants to address that.

2   MS. RICH: Evan?

3   MR. HENDRICKS: Yes, thank you. I think it

4   is because some of the steadiest pollings by Lou

5   Harris and through the 1990s was, "Do you feel like

6   you're losing control of your data," and that was

7   the issue.

8   And, of course, the direct marketing

9   industry is in the business of sending out mail, so

10   they're going to try to refocus the issue there,

11   but the truth of the matter is what's driving this

12   issue is people feel they're losing control of

13   their data, and they don't like it, and they would

14   like something to be done about it.

15   MS. RICH: Fred?

16   MR. CATE: Yes. I think on the education

17   point, of course it's exceptionally well taken. If

18   you write it in language that people don't

19   understand, they're less likely to perceive it.

20   I think, however, the issue goes much

21   farther than that, and I think probably everyone in

22   the room would know it, and if you want to try a

23   test, have The Washington Post when people call to

24   subscribe or to buy classified ads read the first,

25   say, page of their privacy policy on the phone to

1   them, people aren't overly interested.

2   They really didn't want to go on. They

3   want the service. They couldn't care less. Let's

4   move ahead. It might be different if you were

5   going to a doctor or something, very contextual.

6   I understand that, but I think the problem

7   is, is when we talk about transparency, whether we

8   mean notices or that you tell everything you do or

9   you make it possible for them to find it, that

10   there really is a reality that people are not that

11   interested in that they love great stories. They

12   love human interest stories and all of that.

13   But to describe the data processing

14   operation of a corporation, to have anyone do it,

15   the best marketer in the world, I just don't think

16   it can be done.

17   MR. O'HARROW: If I could add one follow up

18   thought, which I think is interesting. One of the

19   things that's interesting here is without a doubt

20   that without a doubt, people love the services,

21   even if they don't know how it's done.

22   There's no question, people are loving the

23   personalized services. They're climbing on to the

24   stuff like crazy, and it's definitely the future of

25   business in our time.

1   Yet, when they find out how that service is

2   provided, and not just necessarily in a human

3   interest story, but let's say an analytical story,

4   they find -- we find that oftentimes they get

5   freaked out, and they're not so sure they like the

6   service under the terms that they've taken it.

7   MS. CULNAN: Jessica, can I add just one

8   quick point? I think we don't really know a lot

9   about sort of the consumer process of learning

10   about this and what really works. We haven't done

11   a lot of research, and I think it's an area where

12   now that we've moved past sort of the, yes,

13   everyone is concerned about privacy kind of surveys

14   that are coming in, is to really do some academic

15   research.

16   What are the trade-offs people make? What

17   kind of notices make sense? I think the idea that,

18   well, notices are too hard to understand so let's

19   not have any notice at all is a bad idea, just my

20   personal preference.

21   There's also a lot of research that's

22   looked at justice, fairness, because this is what

23   this is really about, treating people fairly, and a

24   lot of times people may not want to read the policy

25   or they may not want to exercise their rights under

242

1   some kind of a justice system, but they want to

2   know that they have the rights, and that then makes

3   them more comfortable in participating, and it

4   makes them think things are fair.

5   So even if they don't click on the privacy

6   policy, they may want to see that link.

7   DR. CATLETT: Just to comment on Robert's

8   observation that people like the product but when

9   they found out how it's made, they're not so sure,

10   it reminds me of Prince Von Bismark's remark that

11   the less people know about what goes into making

12   laws and sausages, the better they'll sleep at

13   night.

14   I think that the food analogy is a useful

15   one here. Congress passed the Pure Food Act in

16   1904. It didn't actually say you couldn't put

17   cocaine into the Coca-Cola. They said you just

18   have to label the fact that you're putting it in.

19   And I think that transparency in terms of

20   actually showing us the data about you and what

21   goes into making it is part of enabling consumers

22   to have a real choice about whether they want to

23   buy or participate in that product.

24   MS. RICH: Let's take the next or a few

25   more questions.

243

1   MR. LE MAITRE: I'm sorry, I was going to

2   respond on the point, Am I losing control of my

3   data. My name is Marc Le Maitre. I work at

4   Nextel.

5   I moved to the U.S. about four years ago,

6   and I started from ground zero literally. Nobody

7   had anything on me, including the credit reporting

8   or anything, and the first pieces of mail and the

9   first unsolicited phone calls were actually quite

10   welcome. My wife engaged the gentleman on the

11   phone for an hour and a half. She didn't buy

12   anything but was delighted to receive the phone

13   call.

14   It actually taught me a lot about the

15   community that I moved into, so I actually welcomed

16   it, but it's now got to the point now where I can't

17   sit down in the evenings to dinner with my children

18   without getting an unsolicited phone call.

19   And I think it's got to the point now where

20   I -- at first I knew exactly who it was who was

21   abusing it. The first company I gave my

22   information to was my bank. I will not say which

23   bank, unless you ask me afterwards, but it's now

24   got to the point where I bought a DVD player two

25   weeks ago, and I was getting unsolicited requests

244

1   to join clubs to buy DVDs.

2   And so some of it is good. My question is:

3   Where is it going to end? I don't have a great

4   deal in the way of health information in this

5   country yet, so I still don't know whether that's

6   being abused.

7   Financial information I'm fairly confident

8   is being used without my knowledge, but working in

9   the wireless industry, things like location

10   services, where will it end? At which point do I

11   say, This data is sacrosanct, you cannot have

12   access to it, or will I have the opportunity, or

13   will it just be taken for granted that this is just

14   another piece of information that can be used to

15   market to me?

16   MS. RICH: Does anyone want to respond?

17   DR. CATLETT: Your video rental records

18   are sacrosanct according to Congress.

19   MR. LE MAITRE: But not DVDs.

20   DR. CATLETT: I know the fact that you

21   bought a DVD is not sacrosanct.

22   MR. HENDRICKS: Okay. I think that to

23   answer your question in the short run, no, you will

24   not have that right. I don't there's any realistic

25   chance in the next six months to nine months that

245

1   significant legal protections for privacy and

2   individual's personal information will be passed.

3   I don't think the current power machine and

4   the administration in the Republican leadership is

5   interested, and so I think this is more of a long

6   term struggle.

7   MS. RICH: The gentleman on the left there?

8   MR. BEHRENS: If this is working, I'm Ed

9   Behrens with the Progress and Freedom Foundation.

10   I wanted to follow up briefly on Mr.

11 Miller's comments on providing notice, choice, et

12 cetera, in the interest of serving consumers, but I

13 think there's two dimensions to the question.

14   One is: Should they be provided? The

15 second is: Should they be mandated? And I think

16 that's a separate question.

17   And I would like to draw out the panel on

18 the practical ramifications of mandated principles

19 versus not, both beneficial and adverse.

20   Thank you.

21   MS. RICH: Who would like to respond?

22   MR. CERASALE: Sure, what the hell? I like

23 to use an example of a business model that would

24 not be allowed by the DMA guidelines and decide

25 whether or not we want to outlaw that business

246

```
 1     model.

 2             You go to my Web site, Jerry Cerasale.com,

 3     and the first thing you see, notice, and I sell

 4     radios, so it's a commodity.  I try and sell you,

 5     provide you these radios at the lowest price

 6     possible.  I hold down costs as much as possible.

 7     In that light I share and rent your information to

 8     others and provide the savings on to you.

 9             I do not provide you the opportunity to not

10     participate in this sharing.  I do not provide

11     access opportunity to you because both of those

12     things will increase my costs and therefore

13     increase the cost of my goods to you.  If you don't

14     like this, please, please shop elsewhere.

15             Is that business model illegal?  And that's

16     what most -- a lot of people discussing would make

17     that an illegal business model.  I don't think

18     that's where we should be.

19             MS. RICH:  If people are willing to go a

20     little bit into the break, we could take some more

21     questions, and it looks like everyone wants to ask

22     questions.

23             MR. HENDRICKS:  And, Jessica, just quickly,

24     the OECD guidelines were adopted in 1980 and

25     endorsed by the United States government and all
```

1   Western, European and Japan and Canadian.

2   Yes, I would say we want to see those

3   guidelines incorporated into law across the board,

4   yes.

5   MS. LEGIEREM: (Phonetic) My name is Ann

6   Legierem with a banking agency, and my question's

7   really with as far as I'm a consumer, this morning

8   there were statements made that best practices

9   would have it that marketing associations disclose

10   that you're going to share the information or

11   whatever.

12   And I was wondering if there's any kind of

13   figures that you collect that you really have an

14   idea of how many do really make disclosures to

15   their consumers.

16   And then as a consumer, a mother and all, I

17   saw an article on the CNN Web site recently, about

18   two weeks ago, about how schools had -- the kids

19   were surfing the Internet I think as part of their

20   classroom studies, and there was a marketing

21   company who had software on the computers.

22   They were following the click streams.

23   Well, the parents didn't know about it, but then

24   that, like the dynamic pricing, somebody tripped

25   over it, found out about it, caused an uproar, it

248

1   was pulled.

2   So I guess what I'm saying is this morning

3   representations were made about -- representations

4   were made about, Well, our best practices are that

5   we disclose to consumers but I'm wondering in

6   reality how many really do.

7   MS. RICH: Would anyone like to respond?

8   Jerry's on the hot seat.

9   MR. CERASALE: DMA has a privacy promise

10   that requires disclosure. We have an FTC letter

11   exempting us from antitrust problems as long as we

12   can kick people out. There are 3,000 marketers,

13   3,500 marketers that have signed it.

14   I would say that 80 percent of the mail you

15   receive is probably from members of the Direct

16   Marketing Association, and so we have -- so those

17   are the numbers we've got. We have our own mail

18   preference service, telephone preference service to

19   pull people off of lists.

20   There are well over 3 million names on each

21   of them. They're free to consumers to get on, and

22   so those are the numbers that we have, so the major

23   marketers who are members of ours do direct

24   marketing, which are some of the largest marketers

25   in the country, do provide notice and an

1   opportunity to say no.

2   They in a sense would not follow that

3   business model I just mentioned.

4   MR. LANE: Can I just make a comment

5   getting back to Mr. Behrens' comments about

6   federally mandated laws?

7   I think what this panel has shown, for the

8   most part because it was supposed to be empirical

9   evidence about the effects of mergers and

10 acquisitions or mergers and exchange on consumer

11 businesses, and there are reports that are

12 beginning to come out to highlight what some of the

13 costs are.

14   But I think what we have found is we don't

15 have a lot of information, that we are just looking

16 at the impact that information sharing has on the

17 overall economy. Who is in Mary's first survey on

18 Web sites and who has privacy policies and who

19 doesn't and what impact that has on consumers.

20   We have the Forrester research that says $2

21 billion lost on Internet sales. Are they real?

22 What other information do we have?

23   So from our point of view, what our biggest

24 concern to get to federally mandated legislation is

25 that we don't have enough information on what harms

1   are we trying to address specifically and how those

2   harms -- and the cost benefit ratio of those harms

3   and where really are the American people.

4   We know the American people are concerned

5   about privacy. We all know that. That's why this

6   room is filled. Yet we don't have the details of

7   what are those concerns, the next five layers below

8   that, and I think before we move forward in any

9   federal legislation, we need -- or state

10   legislation -- we need to get a little more

11   dynamics and not the rhetoric that we constantly

12   hear across the board on both sides, but some real,

13   factual data of what are we talking about.

14   And I don't think we're there yet, and this

15   panel is a perfect example. We don't have a lot of

16   facts. We're all saying the same rhetoric that

17   we've been saying for five years now. Yet nothing

18   has improved, but we're beginning slowly to get

19   information, and that's critical.

20   MS. RICH: The gentleman back here?

21   MR. MEISINER: Thank you, Madam Chair.

22   Speaking of facts, my name is Paul Meisiner from

23   Amazon.com. I have to do this stand up routine

24   now.

25   Maybe it's the lack of oxygen in this room,

251

```
1    but I understand it was alleged that we engaged in

2    dynamic pricing last fall.  In fact, there was

3    apparently some long description of how this

4    so-called dynamic pricing was discovered.

5            But let me assure you that policy making is

6    difficult enough based on facts, but when it's

7    based on fiction, it cannot go right.  We did not

8    engage in dynamic pricing.  We never have, and we

9    actually have promised never to do it, even though

10   it would be perfectly legal for us to do so.

11           Let me repeat, back last fall we engaged in

12   some random price tests where we would serve up

13   different prices to consumers based on when they

14   came on.  If you were the same person sitting at

15   the same terminal, same browser, you hit our site

16   several times, you're going to get a different

17   price for the same item.

18           The whole idea was to figure out where to

19   price the item.  Well, random, again based not on

20   demographic information.  It was not a privacy

21   issue, full stop.

22           Well, we got a lot of flack for it and

23   rightfully so.  It confused our consumers, our

24   customers, and we regretted doing it.

25           As a result what we did is we promised
```

252

1   never to engage in dynamic pricing ever again,

2   something that would be perfectly legal for us to

3   do, and then we went and refunded all of our

4   customers, even the ones who had paid willingly 12

5   bucks for a CD.

6   We went and refunded them the difference to

7   the very lowest price, and we said, If we ever in

8   the future ever do this random price testing again,

9   we'll do the same thing so that everyone will

10   always pay the lowest price.

11   Frankly we're being held to a much higher

12   standard than other businesses are being held to,

13   but I think frankly it really pains us all when we

14   have to sit through one of these meetings and find

15   out that what has been discussed here is factually

16   inaccurate.

17   DR. CATLETT: Paul, I don't think I

18   misrepresented that Amazon did the random pricing.

19   I think I said that it was accused of -- we'll have

20   it in the record.

21   MS. RICH: Ted Wham has a quick comment,

22   and then we'll take one more question, and I think

23   everyone wants to splash water on their face, it's

24   so hot in here.

25   MR. WHAM: Ted Wham with Database Marketing

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025

1   for the Internet. I had one quick statistic I

2   wanted to share. I previously worked at

3   Excite@Home, and when I was there, I was the Chief

4   Privacy Officer among several hats that I wore at a

5   rapidly growing company.

6   There was a segment on 60 Minutes regarding

7   Internet privacy. It was approximately two years

8   ago, two and a half years ago. Jason Catlett

9   actually was one of the speakers on that session

10   just describing -- so you hold it closer, it works

11   -- describing the risks to the consumer on the

12   Internet basis.

13   We were asked by 60 Minutes to participate

14   as one of the companies being interviewed, and we

15   originally said yes, and then we went, Oh, God, we

16   don't want to do this, and we said no.

17   And because we additionally owned a

18   third-party ad serving firm, MatchLogic, we were

19   concerned that we were going to be targeted within

20   the segment and wanted to be very prepared, so we

21   went full out and made certain everything was

22   aboveboard, and we went through the privacy policy

23   links, privacy policy on absolutely every page of

24   the site, where they remain I believe to this day,

25   and really tried to make certain that we were

1   ready.

2   The day immediately following the airing of

3   one of the top five most watched television shows

4   in the United States where portions of our site

5   were shown and the risks to consumers of privacy,

6   Excite@Home, as it does every day for the past year

7   or so forth, received over 20 million unique users

8   visiting the site that day. If my recollection is

9   correct fewer than 100 of them accessed our privacy

10   policy links.

11   The notion that consumers want to take --

12   now, you can argue whether the privacy policy that

13   I wrote was easily readable and comprehensible and

14   so forth, but only a hundred people got there to

15   find out.

16   The notion that the consumer is interested

17   in learning about this and spending the investment

18   I think is mistaken. I think the comments that

19   Fred brought up, Fred Cate brought up that most

20   consumers want to have, quote, privacy, don't

21   bother me with the details, is much, much more

22   accurate.

23   MS. RICH: One more quick question, and the

24   gentleman over here.

25   MR. SMITH: Yes, Richard Smith, The Privacy

255

1   Foundation. One thing we're hearing a lot about,

2   how profiling and gathering of consumer information

3   benefits businesses.

4   I've heard very little about cost, other

5   than two very interesting numbers. One person said

6   acquisition costs today for E-commerce sites was

7    $2,000 a customer, which is probably on the high

8   side, but I don't know of really any business,

9   other than maybe the yacht business, that could

10   afford that.

11   And then also the issue of the credit card

12   offers, that the number that are going out is going

13   up dramatically in the last two or three years. At

14   the same time the response rate inversely

15   proportional is going down at the same rate.

16   So I'm wondering here in business how much

17   feedback in the process is really going on. Were

18   these online and data gathering things cost

19   effective really or is it just we're on a sled here

20   and we're heading in this direction and we'll go

21   on?

22   Thanks.

23   MR. LANE: I think a lot of businesses, and

24   if you look at the downturn in ad revenue on the

25   Web sites, as we all know, they're hurting, in the

1   newspaper industry where San Jose Merc is laying

2   off hundreds of people because ad revenue is

3   dropping, and companies are beginning to

4   reevaluate, Is it worth spending $2 million

5   advertising on the Super Bowl.

6   I think there's a wholesale looking at what

7   is the best way to reach out to your customers, and

8   that is the whole goal, but what I think is great

9   though, having said that, there hasn't been a lot

10   of facts in terms of pure data and research from

11   this panel.

12   What I think has been very important, and

13   one of the reasons why I was one who supported the

14   FTC putting this workshop together, was we do have

15   an education process to consumers of how

16   information is used in the economy.

17   And I think the other previous panels were

18   better at doing that than maybe this one, but I

19   think once you have a better understanding, I think

20   there will be less fear, and the trust deficit will

21   be reduced once there is again an educated

22   consumer.

23   And so I appreciate and I wanted to thank

24   the FTC for putting this forth to begin our efforts

25   at having the business community focus our efforts

257

1   on educating consumers on I think these critical

2   issues because they are all about how our economy

3   is going to grow and work in the future.

4   MS. RICH: Thank you.   Finally we're at our

5   break.   If you could keep it at a short break since

6   we did get into the break, maybe five minutes, and

7   then come back, maybe we can try to open the

8   window.

9   (A brief recess was taken.)

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

258

```
 1    SESSION 5:   EMERGING TECHNOLOGIES AND INDUSTRY

 2    INITIATIVES:   WHAT DOES THE FUTURE HOLD?

 3

 4    DANA ROSENFELD, Assistant Director, Bureau of

 5    Consumer Protection, FTC, Moderator

 6

 7    PANELISTS:

 8

 9    JOHN KAMP, Counsel, CPExchange

10    LAWRENCE PONEMON, Founding Board Member,

11    Personalization Consortium

12    BECKY RICHARDS, Director of Compliance and Policy,

13    TRUSTe

14    ARI SCHWARTZ, Senior Policy Analyst, Center for

15    Democracy and Technology

16    RICHARD SMITH, Chief Technology Officer, Privacy

17    Foundation

18

19

20

21

22

23

24

25
```

259

```
 1                     SESSION FIVE

 2    EMERGING TECHNOLOGIES AND INDUSTRY INITIATIVES:

 3               WHAT DOES THE FUTURE HOLD?

 4               -   -   -   -   -   -

 5               MS. ROSENFELD:  Okay.  Everybody, we're

 6    getting ready to start our last panel of the day.

 7    Please take your seats.  Please take your seats.

 8    Thank you.

 9               Welcome, everyone, to our last panel of the

10    day.  I'm Dana Rosenfeld.  I'm an Assistant

11    Director in the Office of the Director and the

12    Bureau of Consumer Protection.

13               Our final panel is entitled emerging

14    technologies and industry initiatives, what does

15    the future hold, which I think will be a very

16    interesting panel.

17               We are going to discuss whether new

18    technologies are emerging that will increase the

19    sharing of detailed consumer data, and also we will

20    focus on what self-regulatatory initiatives are

21    underway to address the privacy of consumer data in

22    the merger and exchange process.

23               Our first presenter today is John Kamp.

24    John is an attorney with Wiley, Rein & Fielding in

25    town and serves as counsel for CPExchange.  He has
```

1   extensive experience in privacy and other

2   regulatory issues through his work of over more

3   than ten years as senior vice president with the

4   American Association of Advertising Agencies, the

5   four As, and from his ten years at the FCC before

6   that.

7   CPExchange Network is a volunteer

8   Consortium of over 90 business organizations. It's

9   dedicated to developing a vendor-neutral open

10   standard to facilitate the exchange of privacy-

11   enabled customer information across enterprise

12   applications.

13   CPExchange facilitates the management and

14   promotion of customer relationships by businesses

15   across industry sectors.

16   Special data elements of the CPExchange

17   specification support the development of privacy

18   policies by companies consistent with Fair

19   Information Practices.

20   And with that, I will turn the podium over

21   to John.

22   MR. KAMP: Thank you, Dana. As I'm

23   bringing this up, I must remind some of you, many

24   of you know that I'm a former college professor,

25   and as such, we former college professors know that

1   there is only one class in the day that's worse

2   than teaching an eight o'clock in the morning

3   class, and that's a four o'clock class.

4   So we're going to make this quick. We're

5   going to keep it lively and go forward from there,

6   and we also, as professors, know that we learn more

7   from our students, and thank you to the FTC for

8   organizing this today because I know that we all

9   have learned a lot.

10   The CPExchange is about consumers

11   generally, and one of the things I think as we've

12   listened today through the morning, we heard people

13   talking about it, was businesses who were doing

14   most of this, but they were doing it in order to

15   reach consumers.

16   And looking at our sort of then and now

17   kind of yin and yang here, this is about long-term

18   customer-focused relationships, about new business

19   processes, but it's mostly about high consumer

20   knowledge, mass customization, multiple channels,

21   proactive, integrated and highly responsive to

22   consumer preferences.

23   We want to know who are our customers, what

24   are their wants and needs, what are the economic

25   value of those needs, and how do we apply that

262

1   knowledge and how do we focus on those consumers.

2   So the successful enterprise interacts with

3   consumers through many channels such as -- and has

4   many opportunities to understand those consumers.

5   The imperatives in all of this, this

6   customer driven, are protection of privacy, the

7   sensing and responding to consumers' needs,

8   satisfying those needs, reducing those costs to

9   consumers and increasing the shareholders' equity

10   of the company.

11   Looking at this, the CPExchange was really

12   designed to facilitate an enterprise's ability to

13   share consumer information internally in large

14   companies. Of course it's gone forward. It's no

15   longer just used, designed for consumers.

16   If you look at this model here, the

17   schematic here, the CPExchange core, the group got

18   together to look at the preferences, business

19   objects, whatever, also added the functionality of

20   the Web, most importantly through Dan Jaye, also

21   someone who is very familiar in these quarters, at

22   Engage Technologies, was part of the FTC Advisory

23   Committee on Access and Security, worked very hard

24   to develop the CPExchange privacy principles, which

25   are P3P compatible, and all this is an XML

1   schemata.

2   Looking at just the privacy declaration

3   component in the P3P compatible, you see in that,

4   you see very specific data elements for purpose,

5   retention and access, and looking just at one of

6   those, the retention component, you can see that

7   there are many data elements that make it possible

8   for this system, this protocol to ensure that there

9   is a face with the consumer.

10   Now, remember, CPExchange is not a data

11   aggregator or a business that's in the business of

12   aggregating these data. It essentially is the

13   development of a protocol that people can use, may

14   use. It's wholly voluntary, can be used by

15   companies for the purposes they wish.

16   But because in this -- in these late data

17   sensitive times, privacy times, it was created

18   during the period that the FTC was looking at these

19   privacy principles and customers were making their

20   preferences so apparent to companies, these privacy

21   elements were contained in it.

22   So quickly our summary slide, CPExchange

23   facilitates that customer awareness and focus,

24   enables corporate privacy policy implementation and

25   addresses the privacy preferences of the consumer.

1   It's platform, vendor and application

2   independent, provides a comprehensive view of the

3   customer and the way that customer interacts with

4   the many facets of the enterprise, provides

5   granular privacy and an authorization model and is

6   designed to promote optimal query and reporting

7   systems.

8   We suggest that you, as you look at this,

9   remember that it's neutral, and it's open, and you

10   also can find more information about it by going to

11   the Web site CPExchange.org.

12   Thank you.

13   MS. ROSENFELD: Thank you, John. That was

14   very succinct.

15   Our next presenter is Ari Schwartz. Ari is

16   a policy analyst at the Center for Democracy and

17   Technology, CDT. His work focuses on protecting

18   and building privacy protections in the digital age

19   by advocating for increased individual control over

20   personal information and expanded access to

21   government information via the Internet.

22   Ari also serves on the advisory committee

23   of the Worldwide Web Consortium and is a monthly

24   columnist for Federal Computer Week Magazine.

25   Ari?

1   MR. SCHWARTZ: Thank you.   This is the

2   first time I've ever seen the windows opened up in

3   this room, and I kind of like it actually.

4   I'm going to talk about how technology has

5   both -- kind of the positive ways that these new

6   technologies can be used to protect privacy.   The

7   story with most of these new technologies is always

8   bad news for privacy and good news for privacy.

9   In this case the bad news is you look at

10   XML technologies, technologies that allow companies

11   to tag information and exchange it more clearly and

12   more openly means that there's greater sharing and

13   that there's going to be greater profiling.

14   Richard Smith will go into this in a little

15   bit more detail, but the good news is that these

16   same technologies open the door for new types of

17   privacy enhancing technologies.

18   I'm just going to give you two examples of

19   this to kind of kick things off.   At CDT we don't

20   build technologies, and that's for other people to

21   come up with those kind of -- these kind of

22   applications, but just to give some ideas of what

23   people have been talking about and what they've

24   been thinking about.

25   The first one is the idea of tagging data

1   collections with a current privacy policy using the

2   P3P vocabulary. John talked about this a little

3   bit, but I'm going to try to explain a little bit

4   more what P3P is and how other technologies can use

5   this.

6   P3P was really designed originally to do

7   business to-consumer transactions, to get at the

8   question that we heard on the last panel asked

9   maybe seven or eight times, about how consumers are

10   having trouble reading privacy policies, that

11   they're seven pages long, that they don't go there.

12   Ted Wham brought up the point that people

13   aren't going to a page. Well, having read many,

14   many, many privacy policies over the past six

15   years, I can tell you that I find them difficult to

16   read, and therefore I know how consumers must feel,

17   that you go to one, you don't really feel the need

18   to go to the next one if you're not going to be

19   able to understand it.

20   The idea of P3P was to allow a consumer to

21   put in their preferences, their expectations of

22   what they want to see out of a site and have the

23   site put in what their privacy policy is. When the

24   browser gets to that site, they match up, and at

25   that point the consumer has more control, and they

1   can decide whether to block that site.   They can

2   decide whether to provide information.   They can be

3   prompted.

4   Really that's up to the browser

5   manufacturer right now, and we're going to be

6   seeing some of these applications in the next few

7   months, but in order to do this, we had to create a

8   vocabulary because we went around looking for

9   vocabularies for privacy that went in to the real

10   details about retention, as John showed us.

11   And no vocabularies existed that really

12   gave kind of multiple choice answers in the way

13   that a Web site would need to be able to describe

14   it if P3P were going to work.

15   So we created this vocabulary.   Let me see

16   if I can get it open now.   I lost the mouse.   Oh,

17   here it is.   This mouse, okay.

18   So this is just the basic P3P vocabulary,

19   and we came up with these questions based on the

20   Fair Information Practices.   The eight Fair

21   Information Practices in the OECD guidelines were

22   the starting point, but we really instead of --

23   because those are really at a high level and we had

24   to go into the detail and answer the multiple

25   choice questions underneath, we worked with -- this

268

1   is a P3P working group, worked with data

2   commissioners in the EU and in Canada, privacy

3   advocates, companies and others, and really built

4   this kind of -- the kind of questions that would

5   need to be answered.

6   But the idea here is that this is -- while

7   this was -- we originally came up with this

8   vocabulary to be used for business to consumers,

9   people quickly found out you can use this for

10   business to business as well, for sharing of

11   information.

12   You can tag this on and use it to help

13   companies audit internally or have third parties

14   come in and audit for them, to set up software that

15   controls the use of information so that you can't

16   send out, put people's Email addresses in the "to"

17   field when it has -- when individuals sign up to a

18   policy saying that their Email address would not be

19   shared.

20   There's a company called Privacy Wall

21   that's building this kind of software right now, so

22   there's a whole bunch of uses for this technology

23   not originally envisioned, but you can use this

24   vocabulary to answer that.

25   Also, there's the ability of access that

1   these new technologies provide. We heard a lot in

2   the last panel again about cost and how cost -- how

3   this was going to be -- that access was too

4   expensive for consumers, this was discussed a lot,

5   to provide to consumers.

6   Well, if companies can provide the sharing

7   between companies and make that less expensive,

8   then they can also make it less expensive to

9   provide it to consumers as well, and we shouldn't

10   be overlooking the fact that making it cheaper in

11   one aspect is also making it cheaper in another

12   aspect.

13   And then the final point here is the

14   question of how this is really going to work and

15   whether there will be market incentives for

16   companies to use this vocabulary, to use the new

17   access features, and that's still really

18   questionable.

19   This is obviously all stuff that happens

20   behind the scenes, and right now responsible

21   companies seem to be taking up these ideas, but

22   will it be wide spread practice? And the answer to

23   that is that we still don't know.

24   MS. ROSENFELD: Thank you. Ari.

25   Our next presenter is Richard Smith.

270

1   Richard is the Chief Technology Officer for The

2   Privacy Foundation, where he directs The

3   Foundation's research activities. He also has

4   primary responsibility for explaining The

5   Foundation's research findings to the media and at

6   public events like this.

7   Richard?

8   MR. SMITH: First of all, I want to thank

9   the FTC for inviting me to speak today, and I was

10   asked to actually look into the crystal ball here

11   to see where technology is heading in terms of

12   sharing more data, this idea of emerging

13   technologies increasing the sharing, and very

14   fortuitously yesterday, Steve Ballmer, the CEO of

15   Microsoft Corporation, gave a speech for the

16   Association of Computing Machinery, that's sort of

17   like the Bar Association for the lawyers in the

18   group here, gave a talk about XML which was going

19   to be my topic so I thought that was very good.

20   And I would like to quote from the article

21   that ZDNet wrote which said that XML as the lingua

22   franca of cyberspace would affect -- and it would

23   effectively clear away lingering barriers blocking

24   companies from exchanging information over the

25   Internet. And then the article goes along to talk

271

1   about the tools that are being developed to support

2   XML and so on.

3   What I found very interesting was there was

4   really no discussion of what kind of data is going

5   to be going back and forth, and pretty obviously

6   some of it is going to be about widgets, about

7   cars, packages and whatever, but it also is going

8   to be personal information, so the answer here,

9   looking into the crystal ball, is clearly yes,

10   we're going to see more sharing because tools are

11   being developed to make it easier to do.

12   There's nothing magical about XML. It's a

13   particular specification of how companies agree to

14   communicate data from one place to another, just

15   like English is a way that humans communicate.

16   The nice thing about it, it's very easy to

17   understand, and it's also human readable, so for

18   folks like myself who kind of like to look at

19   privacy practices of companies, it's actually going

20   to make it easier to look into things, but clearly

21   we're going to see it's -- XML is going to help in

22   the sharing of data, but it's also going to help in

23   some of these areas like P3P and CPExchange,

24   providing some privacy controls.

25   The question is is, Will they be

272

1   implemented? Just because they're in a

2   specification there's still the issue of, Will they

3   be implemented.

4   Now, another issue, if you want to predict

5   the future, I believe in looking in a crystal ball,

6   you have to also follow the money. We first follow

7   the technology, but then we also follow the money.

8   And pretty clearly in the Internet I think

9   the most ardent cheerleader would now say that

10   we've had a dot com meltdown of companies literally

11   wasting billions of dollars on business models that

12   are not going anywhere.

13   But one thing is very clear is that the

14   Internet is a very good place to get information on

15   things. If I wanted to go to the Google Search

16   Engine, I could get information about anyone in

17   this room probably, except for myself because I

18   have a common name.

19   But if you have a not so common name, it's

20   a lot easier to find out information, and I think

21   that really shows a good business model here, which

22   is the idea that people are going to go to the

23   Internet to make purchase decisions but then go to

24   the offline world and buy stuff, like buy a car.

25   And so I really see that as sort of the

273

1   money starting to focus people and business models

2   in that direction, and what that's going to mean is

3   the people that provide the information on the

4   Internet are going to want a piece of the action

5   when the sale is made in the offline world.

6   So I see technologies like XML and

7   CPExchange being done for that, so let me give you

8   a quick example here. We've all bought cars, and

9   it's always an interesting experience. Now that

10   I'm older, I actually feel fairly confident about

11   going in the showroom but at a younger age, it was

12   sort of like me against them, and they had the

13   information, and I think that's going to get more

14   interesting here.

15   For example, we go to a car Web site,

16   research three different models of cars that we're

17   interested in, and the Web site remembers that

18   information.

19   Well, the fun thing is going to be I

20   believe in the future is you can walk into the car

21   dealer. They ask for your driver's license in

22   order to do a test drive, and the other thing

23   they're using that for is to go find out what

24   you've been researching on the Web here, for what

25   kind of cars you're interested in.

1   And that gives the salesman one up on you,

2   which is he knows the other competitive models

3   you're looking at, and he can have computer

4   software that recommends how to sell against these

5   cars. You can also be scored on the likelihood of

6   buying a particular model that you express interest

7   in and so on.

8   So I think we're going to see this very

9   strong economic push, and I think it's basically

10   inevitable that when we have one part of the market

11   which seems to be dollar poor and another part of

12   the market where the money is being spent, that the

13   business models are going to have to go that

14   direction.

15   And we're going to see -- be forced into

16   more information sharing. It's just an inevitable

17   part of this economics, much more so than we've

18   seen on the Internet itself.

19   Thank you very much.

20   MS. ROSENFELD: Thank you, Richard.

21   Our next panelist is Lawrence Ponemon, who

22   is the president of Guardent, a services and

23   technology company enabling security, privacy and

24   data protection.

25   Prior to joining Guardent, Larry was the

1   founder of the PricewaterhouseCoopers global

2   privacy practice. Larry is a founding board member

3   of The Personalization Consortium, and he will talk

4   about that organization today.

5   MR. PONEMON: Thank you. Everyone looks

6   really hot and really tired. Is that true or is

7   that just a perception that I have? I need to

8   personalize on you.

9   How many people worry about personalization

10   and privacy? Raise your hand. Oh, come on. I

11   know it's late, everyone. How many people worry

12   about personalization privacy in the wireless Web?

13   Let's see if we can get those hands a little bit

14   higher?

15   Quite frankly, there is actually a lot to

16   worry about, in my opinion, and I know I sound like

17   a heretic as a founding member of the

18   Personalization Consortium. I have good news. I'm

19   going to be fast in my presentation, and I do not

20   have Power Point slides so you can actually watch

21   me.

22   The bad news is I'm going to read to you

23   our blurb about what the Personalization Consortium

24   is, and I'm going to tell you where we are and what

25   we are trying to achieve.

276

1   The Personalization Consortium is an

2   international advocacy group formed to promote the

3   development and use of responsible one-to-one

4   marketing technology and practices on the worldwide

5   Web.

6   The Consortium encourages the growth and

7   success of electronic commerce that delivers the

8   benefits of personalized electronic marketing while

9   articulating best practices and technologies that

10   protect the interest of consumers, and I want to

11   underscore consumers.

12   To achieve its goal of expanding the scope

13   and use of personalization technology that respects

14   consumer privacy, the Consortium has many

15   functions, for example, to provide a forum for

16   industry discussion and information, sponsor

17   research, foster standards for technology and best

18   practices and work towards consumer understanding.

19   And toward this end the Consortium has established

20   ethical information and privacy management

21   objectives that articulate its goal to create a

22   solid process that enables consumers to confidently

23   use personalization technology for their benefit.

24   Now, the Consortium was established about a

25   year ago chaired by Don Peppers and a few other key

 1   folks. I was co-oped into joining the Consortium

 2   because of my very strong and very weird views on

 3   privacy. So like you, I was pretty suspicious.

 4   So I attended my first board meeting, and

 5   at the first board meeting were about 30 or 40

 6   company representatives, and I saw a sincere

 7   interest to do it right, and I had this kind of

 8   vision in my mind.

 9   If someone could invent a cigarette that

10   didn't cause cancer, wasn't habit forming, maybe it

11   won't be so bad to smoke, right, and maybe that's

12   where we are in the evolution of personalization.

13   It's probably a bad analogy unfortunately, unless

14   you're a smoker.

15   But the idea is that we've grown from a

16   small group of good companies to 67 great

17   companies, and there are many, many other companies

18   that are taking a wait and see attitude.

19   Let me tell you a little bit about some of

20   the challenges. First, we set high standards. If

21   you read the Personalization Consortium and you go

22   to our Web site which is www.Personalization.org, I

23   don't know how to spell personalization, but my

24   friend Jason can spell it for you. And I think at

25   the end of the day though when you go to that Web

1   site, you're going to find that these principles

2   are about equal, not better than, not worse than,

3   but about equal to many wonderful statements about

4   privacy.

5   So then you scratch your head and you say,

6   "What's the difference here." The difference is

7   we're basically holding our members to a very high

8   standard. That is, it's not just good enough to

9   say you're going to comply with these principles,

10   but you have to undergo an audit, the A word,

11   audit.

12   And that's pretty scary because if you're a

13   small organization or a large organization and you

14   say you're going to be a member and suddenly you're

15   no longer a member, you're basically killed or

16   kicked off the membership list, it's a signal that

17   basically suggests -- not suggests, that tells the

18   universe that the company failed to comply.

19   Let me just tell you the courage of

20   members. The founding members are very courageous

21   because right now they just generally assume that

22   they're going to pass this audit, but my guess is

23   many will fall by the wayside and that the end

24   result will be that some members will not make the

25   grade.

1   Now, let me just tell you it's not for pure

2   altruism, it's not because we're good guys.

3   There's a real economic value proposition,

4   something a little bit different than regulation

5   and lawsuits, and that is if we do it right,

6   becoming a member is going to be a good thing.

7   It's going to be something that is of great value.

8   It's going to be a way to differentiate your

9   services and product in this ever evolving

10   marketplace.

11   Now, if that's so, then people will knock

12   the door down to become a member. To become a

13   member will have real substantive meaning, and

14   that's really what we're trying to achieve through

15   the independent verification.

16   Also, some people are confused, and the

17   next speaker will talk about TRUSTe. The next

18   speaker will also discuss the issue of seals. This

19   is not just a seal. It's not a new form of a seal

20   program. It is in fact about an independent audit

21   conducted by a trusted party.

22   So that's all I want to say about the

23   Personalization Consortium. I'm very proud to be a

24   member, even though I was co-oped to becoming a

25   member originally. It's a great group, and I

1   really encourage everyone here, as well as in the

2   spillover rooms, to go to our Web site and to find

3   out more about what we are and what we want to

4   become.

5   Okay so without further ado, I'll sit down.

6   Thanks.

7   MS. ROSENFELD: Thanks. Thank you, Larry.

8   Our next panelist is Becky Richards. Becky is the

9   Director of Compliance and Policy for TRUSTe, an

10   Internet privacy seal program. She oversees all

11   aspects of enforcement operations and policy

12   developments for the TRUSTe program, including

13   TRUSTe's compliance operations and the TRUSTe Watch

14   Dog Dispute Resolution Process.

15   Prior to joining TRUSTe, Becky was an

16   international trade specialist on the electronic

17   commerce task force at the U.S. Department of

18   Commerce's International Trade Administration.

19   Becky? That's a mouthful.

20   MS. RICHARDS: It is a mouthful. I don't

21   have a Power Point presentation either, so being

22   the last person to speak on the last panel, I hope

23   we'll get through this quickly.

24   I'm actually not going to really talk about

25   seals today. Most of you probably know what they

281

1   are.   Instead, I'm going to talk -- we've heard

2   today a lot about merging and exchanging of

3   consumer data and what the benefits are and what

4   the risks are.

5   And at TRUSTe, we've been following the

6   practices of merging and exchanging consumer data

7   closely, but TRUSTe's main focus in the past has

8   been on the explicit and inexplicit collection of

9   information from consumers and the sharing of such

10   information.

11   TRUSTe's monitored the increasing practice

12   of merging and exchanging and has been and will

13   continue to work to ensure that consumers are aware

14   of these practices.

15   Mary Culnan in the previous panel brought

16   up a very good point.   Transparency is very

17   important.   If we're going to continue to increase

18   growth via E-commerce, we need to have consumers'

19   trust, and trust comes through transparency and

20   understanding of what those practices are.

21   Currently because we've really been looking

22   at how information is collected from the consumer

23   as opposed to the other way around, our license

24   agreement doesn't -- does not explicitly address

25   the disclosure of merging and exchanging of

282

1   information, although depending upon the practices,

2   it could be required.

3   As we look to the future, we will

4   explicitly require companies to disclose the

5   practices of merging and exchanging information, to

6   increase the transparency and to increase trust.

7   Our current practices are that we ask Web

8   sites whether they're combining information from

9   third parties by asking in the self-assessment," Is

10   your company supplementing the information that you

11   receive directly from users with information

12   received by an offline means or from a third-party?

13   If so, explain."

14   So if a Web site states that information is

15   being supplemented from such sources, this should

16   be disclosed in the privacy policy.

17   TRUSTe has a model privacy statement that

18   is currently used by a number of companies as a

19   privacy resource, and in this model privacy

20   statement, we provide two different examples of how

21   a company can address the supplementation of

22   consumer information from third parties.

23   The first example is really more

24   appropriate for gathering of financial information,

25   and so I won't go over that specifically.

```
 1        Our second example deals with the combining
 2   of marketing information with consumer information.
 3   It states:  "In order for this Web site to enhance
 4   its ability to tailor the site to an individual's
 5   preference, we combine information about the
 6   purchasing habits of users with similar information
 7   from our partners, Company Y and Company Z, to
 8   create a personalized user profile."  So this is
 9   the disclosure.
10        Now, for perhaps maybe a more real world
11   example.  I have three examples.  The first one is
12   one of our licensees that states explicitly that
13   they do not supplement consumer information by
14   stating that all information excluding our user
15   passwords originates solely from our primary
16   client.
17        Now, in the case of a company that does
18   supplement consumer information, one of our
19   licensees states:  "We may research demographics,
20   interests and behavior of our customers based on
21   the information provided to us upon registration."
22        And finally, a third example that gets
23   lengthier; and as we've discussed, privacy policies
24   can be rather long:  "The combination of offline
25   and online information provided by the customer has
```

1   the ability to enhance the customer experience and

2   make customers' interaction more meaningful and

3   relevant. Company X requires that any consumer

4   profiling or purchasing behavior captured online

5   and combined with offline information be clearly

6   stated to the consumer at the time of the online

7   data collection. The consumer will have the

8   ability to choose not to be part of a subsequent

9   marketing campaign."

10   So in this last disclosure, the company is

11   giving the individual the opportunity to opt-out of

12   being profiled.

13   I would like to thank the Commission for

14   having today's workshop. I think it's been very

15   informative as to both the benefits and risks

16   involved in merging and exchanging information

17   across businesses.

18   The important part of each of these, in

19   thinking about this for both businesses and

20   consumers, is that the consumer needs to be

21   informed of the practice if we are going to

22   continue to increase transparency and trust and

23   continue to see increase in business on the

24   Internet.

25   And as I mentioned at the beginning, TRUSTe

285

1   will be changing our license statement to

2   explicitly address this particular practice in the

3   future.

4   Thank you.

5   MS. ROSENFELD: Thank you, Becky. I have a

6   few questions, we want to try to stick to the time

7   frame here, and then we'll open up the floor to

8   questions from the audience.

9   John, we know CPExchange is an open and

10   it's a voluntary standard, and I think that means

11   that the privacy related features also have to be

12   voluntarily adopted by the users.

13   How likely is it that companies are going

14   to deplore the privacy-related features of the

15   specification in your view?

16   MR. KAMP: I hope they don't deplore them.

17   It is getting late though.

18   MS. ROSENFELD: Did I say deplore?

19   MR. KAMP: Deploy.

20   MS. ROSENFELD: I'm sorry, the heat is

21   getting to everyone here.

22   MR. KAMP: We don't know. In fact, we have

23   reason to believe that they don't deplore them,

24   that they will deploy them, but because it's a

25   voluntary standard, as Jason once described it,

1   it's a safety that may or may not be used.

2   We expect though, because remember the

3   whole point of all of this day has been businesses

4   are interested in customization because consumers

5   are demanding it.

6   As consumers demand more and more privacy

7   transparency, the privacy transparency will be used

8   by the successful companies, and they will use that

9   part of the CPExchange protocol.

10   MS. ROSENFELD: Is there any effort

11   underway to develop a code of best practices for

12   those users of the specification?

13   MR. KAMP: We worked first of all to make

14   sure it was P3P compatible because we believe

15   that's really very important, and we have, just in

16   the last week, sat down again with the P3P people,

17   CDT, and are exploring alternatives, ways in which

18   we can continue to ensure that the protocol is as

19   multifunctional in this regard as possible and will

20   be looking at those very kind of things going

21   forward.

22   MS. ROSENFELD: I guess on a related note,

23   in terms of being multifunctional, will the

24   specification be used to facilitate merger and

25   exchange of consumer data across media, for

287

 1   example, into wireless space?

 2   MR. KAMP: Again, it's a neutral protocol.

 3   It was designed for internal data sharing within

 4   companies, and as we went forward, we added the

 5   other functionality.

 6   My guess is that all of the things that

 7   will be possible and will be used by companies are

 8   likely to use this protocol because we think that

 9   it's valuable in that regard, and, yes, it could

10   very well be used for wireless or whatever other

11   scary things that might happen in privacy going

12   forward.

13   But because of the kinds of focus there has

14   been on privacy by this agency and others going

15   forward, I'm convinced that the American public are

16   learning what privacy is all about and learning how

17   to use, how to make their choices, and that those

18   kinds of things will automatically develop as the

19   industry develops.

20   The important point here is not that the

21   functionality will be required, but that it's built

22   into the system so that it can be used and the

23   commitment by CPExchange to make sure that the

24   system does have that functionality.

25   MS. ROSENFELD: Go ahead, Ari.

1   MR. SCHWARTZ: In terms of functionality of

2   CPExchange and whether that alone will spur

3   individual -- spur companies to use it, I do think

4   that the regular P3P that I was talking about

5   earlier in terms of Web sites, Web browsers going

6   to Web sites and seeing whether they have privacy

7   policies that match consumers' policy, that has a

8   -- direct impact on the consumer.

9   There's direct feedback that a consumer

10   will want to see a privacy policy because it will

11   show up in their browser. CPExchange doesn't have

12   that ability to be right in the consumer's face

13   like that, so there is that missing step there.

14   It really does have to be a responsible

15   company to take that on, and I look forward to

16   working with the CPExchange people, but we have to

17   recognize that there is that missing piece with all

18   of this behind the scenes type transaction.

19   MS. ROSENFELD: Larry, can you just

20   describe the kinds of companies that are members of

21   the Personalization Consortium and what kinds of

22   companies you expect will join in the future?

23   MR. PONEMON: Good question. Of our

24   members today, we have a combination of tool

25   makers, people who are inventing new technologies,

1   both in the wired and the wireless area, and

2   they're the largest chunk of members.

3   We also have vendors, companies that are

4   not actually making the technology but selling that

5   technology or embedding that technology into other

6   tools, so for example in the CRM universe we see

7   companies fall into that space.

8   Then we have end users, companies that, for

9   example, like AMR, American Airlines or Charles

10   Schwab, that are actually the users of this

11   technology.

12   If you kind of think about the model, the

13   model is a little bit weird because it's a

14   B-to-B-to-C model. We're adding now a new element,

15   and so the key is to get to the consumer.

16   Even if you are in a business mode, and you

17   personally -- as an organization you do not have

18   direct access to personal information, there's

19   still a chain of trust and responsibility, and

20   that's really what the audit is attempting to

21   prove.

22   So you can't say," Well, we passed but

23   guess what, the audit was simple because we don't

24   have personal information, we don't collect any

25   information because we're a tool maker." You can't

290

1   get away with that.

2   That's obviously a very slippery slope, but

3   that's not what the audit is about, so the members

4   are primarily in those three categories, and we're

5   really -- to answer your question about what is the

6   future, if you'll look at all of the users of

7   personal information, there's a huge body of end

8   user organizations that would love to learn more

9   and become a member and to make sure that they're

10   using the technology that is ethical and that is

11   being managed at a high level.

12   Unfortunately to get there, we really have

13   to have those rigorous standards in place, and it's

14   ultimately the responsibility of the tool maker to

15   ensure that the process is a fair one, is a good

16   one, and so we would encourage end users as well as

17   tool makers and vendors to participate in this

18   process.

19   MS. ROSENFELD: Thank you. What about

20   enforcement with the guidelines?

21   MR. PONEMON: You had to ask the

22   enforcement question, end of the day, we're all

23   sweating here. Now I'm really sweating.

24   Basically if you don't comply with this,

25   and you know my favorite word, we're going to kill

291

1   our members. We have a license. They've agreed

2   to -- no, we're not going to kill our members, but

3   what we're going to do is you're going to get

4   kicked off the membership scroll.

5   And we're actually in the final stages of

6   establishing a disclosure standard. While it has

7   not been defined as yet, the plan is to have a

8   status report on our Web site to show where members

9   are in the auditing process, so obviously if you're

10   not there, if you mysteriously disappear one day,

11   you could reach your own natural conclusion.

12   But understand that enforcement is very,

13   very important for this to work. Without

14   enforcement, it is a wasted effort. It is

15   virtually a wasted effort, so self regulation means

16   that the organizations that have become members

17   have to work hard to maintain their membership, and

18   enforcement is going to be very costly for some

19   organizations that don't make the grade.

20   MS. ROSENFELD: Becky, you talked about

21   TRUSTe intending to revise your licensing

22   agreements to require disclosures about data merger

23   and exchange of information, and I'm wondering if

24   you have a time table for that.

25   MS. RICHARDS: We last updated ours I think

 1   in August, September, and I'm told that the legal

 2   fees have to stay lower so I'm not supposed to give

 3   it to our lawyers for a couple more months, and we

 4   also want to have a certain level of stability in

 5   the program.

 6   And we're actually on the sixth version

 7   right now, we'll be going to the seventh, and there

 8   will be a number of revisions, not just this one

 9   but also to sort of-- what we have done always is

10   to follow along what the privacy debate is, where

11   are we going with things and make sure we're a step

12   ahead.

13   And so I think that we can anticipate to

14   see those sometimes in the July/August time frame

15   as we move forward.

16   MS. ROSENFELD: I think now I'm going to

17   open up to audience questions. The gentleman back

18   there, and again please identify yourself and your

19   organization.

20   MR. LE MAITRE: Hi. I'm Marc Le Maitre. I

21   work with Nextel Communications.

22   Larry, I agree absolutely, entirely with

23   you that privacy without enforcement doesn't fly.

24   During the B-to-B world, very few businesses would

25   do anything without signing a contract, and I'm

1   aware that P3P is policy based, no need for a

2   contract in P3P, how do you get from policy based

3   to contract based so that you've got some basis on

4   which to place -- to put some enforcement around?

5   MR. PONEMON: You're asking a very good

6   question, and we've tried to address this over the

7   course of the last few years, especially with my

8   involvement with the FTC and the Advisory

9   Committee.

10   Quite frankly, one of the problems you have

11   is a policy, doesn't necessarily suggest truth, so

12   you have a lot of organizations that are very quick

13   to post a policy, and P3P by the way is kind of an

14   offshoot of that.

15   P3P is good, but unless you have an ability

16   to say, Okay, you have this policy, how do we know

17   you're complying, it's kind of an interesting

18   problem because a lot of organizations aren't

19   really evil and they're really not trying to dupe

20   the consumer. It's not that at all, but they're

21   not actually digging deep enough into their own

22   business models or into their own organizations to

23   determine where they have vulnerability and risk.

24   And in many cases, in most cases

25   unfortunately, the legacy of being an auditor,

294

1   right, you basically stumble on some incredible

2   problems. Bad news doesn't necessarily get up to

3   the right people. That's the job of an auditor is

4   to communicate it ultimately to the board, and I've

5   been in many board meetings to say to major

6   companies," You know what, what you say you do on

7   privacy, you're just not doing, and it's going to

8   be very costly to fix it."

9   So then that's the other issue. What's the

10   accountability on the other side to actually now

11   fix the problem now that you have that information.

12   Audits are a good thing though. If there's

13   self regulation you might be able to move the bar.

14   MR. LE MAITRE: I think there's some

15   direction on it. The notice and choice aspects of

16   Fair Information Practices are well understood. My

17   own feelings are that it may take some sort of

18   binding between notice and choice.

19   This is the notice you gave me, this is the

20   choice I gave back to you, and some notion that

21   that forms a bond, a contract, that has some legal

22   status that we can both rely upon in an audit

23   situation.

24   MR. PONEMON: Can I just make one comment

25   about that? If you just look at the current

1   implementations around GLBA, Gramm Leach Bliley,

2   we've seen a lot of organizations having a very

3   difficult time just operationalizing choice. We're

4   starting to see evidence that companies are

5   failing.

6   They're getting the reply back, but

7   companies are having a difficult time making sure

8   that it sticks in their legacy systems, and they're

9   spending virtually no resources to fix the problem,

10   so I think we're going to have a lot of interesting

11   issues on the horizon in terms of lawsuits,

12   organizational culpability, but that's a problem.

13   And so even if you have a contract, even if

14   it's a legally binding contract, I'm not sure

15   that's going to change behavior in the short term.

16   MS. ROSENFELD: John?

17   MR. KAMP: I just wanted to mention, and

18   not in any way to slight the FTC enforcement

19   authority or even the authority of auditors, that

20   perhaps the most important thing that will happen

21   in the marketing space is happening, and that is

22   privacy is becoming part of the brand, and as part

23   of the brand, it's part of that image of the

24   product and the company that is part of the

25   relationship that the customer has with the brand,

296

1   and either a company is going -- going forward, I

2   think either companies are going to respect the

3   privacy of their consumers and treat them

4   appropriately or they're not, and that consumers

5   are going to take it out on them, and that the

6   value of the brand and the need to ensure that the

7   brand stands for something in the privacy space as

8   well as in the basic historical places where it

9   talks about quality, product quality and

10   consistency and value proposition, that privacy is

11   going to stand along that, and the American

12   consumers are going to make sure that their privacy

13   is protected in ways that they consider

14   appropriate.

15   MS. ROSENFELD: You in the back.

16   MR. KAMINSKI: Hi. My name is Jim Kaminski

17   from Arent Fox. This is a question for Ms.

18   Richards. I was wondering if you had a sense -- I

19   have two questions actually. My first question is:

20   Do you have a sense of what the industry practice

21   is for disclosing the company's enhancement

22   practices, and also when that new standard is in

23   place, are you going to require the companies to

24   provide access on the Web site to the data

25   collected offline to keep that parallel?

1   MS. RICHARDS: The lovely question access.

2   This is always difficult to answer. Let me maybe

3   revise a little of how I answered Dana's question.

4   Right now there isn't an explicit

5   requirement for you to disclose, but if we go

6   through your privacy practices and we find that

7   it's very appropriate and you should be disclosing

8   it, we will force you to disclose that information.

9   So it's sort of an implicit requirement if

10   you could have that, and so -- and what we have

11   been working with our account managers is to make

12   sure that they know this is an important aspect and

13   they need to be probing more about the questions,

14   and so I think on that aspect it's something that

15   we're -- as the practice becomes more prevalent,

16   we're seeing more disclosures.

17   When I asked the question around the office

18   of if they can give me some different examples, we

19   came out with some different ones, and it was a

20   really good learning experience for everybody to

21   see what is happening.

22   I would say that there's -- I can't give

23   you any numbers in terms of how prevalent it is or

24   how not prevalent it is in terms of how many

25   companies are doing it at this point. It's just a

1   sense that it's definitely increasing and that it's

2   something we're addressing as we go along.

3   I don't have a good answer for your access

4   question at this point.

5   MS. ROSENFELD: There in the middle.

6   MR. TUROW: Joe Turow from the University

7   of Pennsylvania. I just wanted to know if anyone

8   has a sense of whether what you guys have been

9   talking about is going to change when things go in

10   the not too terribly distant future to a much more

11   broadband, very dynamic environment where people

12   will be watching television, doing the Web stuff,

13   doing this, constantly moving between sites at such

14   a rapid speed with so many parties involved in a

15   transaction that the kind of privacy policy issues,

16   I'm just wanting to know, might be totally

17   irrelevant, the ones that we've been talking about.

18   If you have four or five parties that have

19   an interest in dealing with the data at the same

20   time who have very different notions of what's

21   acceptable, is that a scenario that's realistic,

22   and then what do you do?

23   MS. ROSENFELD: Would anyone like to take a

24   shot at that? Ari.

25   MR. SCHWARTZ: Well, I was just about to

1   say that's why XML technology, people are focusing

2   on XML technology, because it's really the only

3   realistic way the different parties can come in at

4   different points, and that's why I focus so much of

5   my time on P3P because I see it as the only

6   realistic way to provide notice in that realm.

7   Now, obviously Larry brought up the point

8   that P3P has a weakness that it doesn't do

9   enforcement. P3P, that's not what P3P was meant to

10   do. It's not supposed to do enforcement. It's

11   supposed to do notice and do it well, and that's

12   what we've tried to focus on.

13   So of course tying in all these access

14   points is going to make it very difficult for the

15   consumers to follow, it's difficult enough to

16   follow on the Web the way they do it today. In a

17   pervasive computing environment only XML

18   technologies will help do that so we need to map

19   everything to some --

20   MR. TUROW: Can you explain how? I don't

21   see how it's helping to solve the problem.

22   MR. SCHWARTZ: How will XML help to solve

23   it?

24   MR. TUROW: Yes.

25   MR. SCHWARTZ: Well, what's going to happen

1   is that you'll have -- it's a complex system, and

2   there's a few different ways that schemas will

3   work, but basically that everyone will be relating

4   to the same basic vocabulary or schema, and then

5   information will be flowing into points back and

6   forth using this same underlying data, using the

7   same tags.

8   So that we don't have the confusion that we

9   have today where everyone has different databases

10   labeled in different ways and uses the information

11   in different ways. It's a whole new infrastructure

12   that Tim Berners-Lee from the World Wide Web

13   Consortium calls the semantic Web.

14   MS. ROSENFELD: Jason?

15   DR. CATLETT: I have a quick question for

16   Larry. Does the Personalization Consortium require

17   its members to provide access to consumers about

18   the data they hold, and does it require an

19   opportunity to delete the information?

20   MR. PONEMON: That was probably again one

21   of the most contentious issues with our principles,

22   but we ruled. We prevailed. Basically access and

23   accuracy are actual principles, and that means that

24   you have to provide access, reasonable access which

25   means that -- I don't like that word reasonable

1   because it opens up for interpretation.

2   We're going to have to be really smart as

3   auditors in terms of finding what's the line

4   between reasonable and unreasonable, but more

5   importantly, if someone finds a problem, you have

6   to be able to provide that individual the proper

7   approach for fixing those problems as well as

8   redress if that is not being handled well.

9   But also this is opening up a can of worms

10   in terms of security and authentication issues that

11   have to be built into the system. From that point

12   of view it could be very costly to members, but

13   that's just what we have to do.

14   DR. CATLETT: But it was a requirement that

15   was accepted by the 67 companies.

16   MR. PONEMON: All but one company agreed to

17   it, and that one company basically has agreed to go

18   along with it so it was amazing, but it was a

19   battle. It wasn't like, Gee, it makes a lot of

20   sense. It had to be -- it took weeks and months,

21   as Win knows, a lot of work to kind of get us to

22   that point.

23   MS. ROSENFELD: Any other questions? No.

24   I want to -- was there anybody else? No?

25   I want to thank the panelists. This was an

1   excellent panel, and it's not over yet. I want to,

2   first of all, commend all of you for staying

3   throughout the day. I apologize for our air

4   control problems, but after this panel can step

5   down, we have some closing remarks by Joel Winston.

6   (Applause.)

7   MR. WINSTON: I think it's fitting that we

8   were able to get these curtains and windows open,

9   because the purpose of this workshop was to shed

10   some light and bring in some fresh air on a very

11   important subject, data merger and exchange, and I

12   hope we were able to accomplish that today.

13   I did notice that it took a crow bar to get

14   some of those windows open, and I don't want to

15   carry the metaphor too far, but actually I think

16   people were very open and honest with us, and we

17   really appreciate that.

18   I want to thank all of our panelists today

19   and our audience for a very lively and interesting

20   day. I also want to express my appreciation to the

21   FTC staff who really worked tirelessly to put this

22   workshop on and to do so really in record time.

23   Specifically I want to thank Martha

24   Landesberg, Allison Brown, Jessica Rich, and Ellen

25   Finn from the Financial Practices Division, Lou

1   Silversin from the Bureau of Economics, and Dana

2   Rosenfeld from the Bureau Directors Office, and of

3   course our intrepid team of support staffers who

4   really made this possible today.

5   Let me just close with a few brief remarks.

6   The Commission's been studying online data

7   collection for over five years now, and we've

8   hosted several workshops on a variety of topics

9   related to collection issues, but I think the

10   subject matter of this workshop is an especially

11   timely one. It seems like every day we hear or

12   read about new ways in which consumer data are

13   being collected and combined and put together for

14   various purposes.

15   It's been a very educational day for us and

16   we hope for all of you. Although some of the

17   practices we've heard about today are practices

18   that have been going on for many decades, new

19   technologies and other recent developments have

20   increased the speed and amount of data that

21   businesses exchange both online and offline, so

22   being able to discuss these practices really helps

23   us keep up with all of these recent developments.

24   We learned today, for example, about

25   various sources of consumer data used for creating

304

1   profiles such as public records, census data,

2   survey data, warranty cards and consumer

3   transactions.

4   In addition, many companies described their

5   business models and how the merger and exchange of

6   data benefits both the businesses and consumers.

7   For example, by purchasing third-party data,

8   companies are able to target their advertising more

9   effectively and efficiently and to personalize Web

10   content, so that consumers may get more advertising

11   that they want to see and fewer advertising offers

12   that they don't want to see.

13   Several panelists raised questions about

14   the transparency of these practices to consumers,

15   in particular, whether consumers know about the

16   existence of data compilers and the practice of

17   enhancing consumer information with data from

18   third-party sources. Do consumers know how and why

19   this data is exchanged between companies?

20   Well, I would harken back to what

21   Commissioner Swindle said this morning and many of

22   the panelists raised throughout the day, this

23   notion of the trust gap and the information gap,

24   the misunderstanding gap.

25   From what I heard today it seems like the

305

1   key problem here is that there's a gap between what

2   businesses are actually doing in their collection,

3   merger and exchange of data versus what consumers

4   think they're doing.

5   I haven't seen any specific survey

6   evidence, and I would certainly welcome it, but I'm

7   willing to bet that most people either dramatically

8   underestimate or dramatically overestimate the

9   scope and detail of information that businesses are

10   compiling about them.

11   On the one hand, I suspect that there are

12   lots of consumers who really have no idea that

13   hospitals and government offices and bankruptcy

14   trustees and lots of other people are selling or

15   providing personal information to businesses, all

16   of which may be combined and enhanced in various

17   ways to form consumer profiles.

18   On the other hand, I imagine there are lots

19   of consumers who think that their every action is

20   being traced, recorded, combined and deposited into

21   some mega database for anyone to use and see. What

22   I heard today is that the information that's

23   actually being compiled and combined out there is

24   not nearly that comprehensive or nearly that

25   granular.

306

1   To me this raises a real challenge. Alan

2   Westin did a survey several months ago on consumer

3   attitudes toward privacy. He found that there are

4   a fair number of people who simply don't want their

5   information shared or used by anyone for any

6   reason.

7   On the other side of the equation, he found

8   that there were some people who really didn't care

9   about their information. They were happy to allow

10   it to be used for any purpose whatsoever. But,

11   what he also found is that there are about

12   two-thirds of the survey participants who fit into

13   the category of what he called privacy pragmatists;

14   that is, people who are willing to share their

15   information under certain circumstances for certain

16   reasons and if they're promised certain benefits.

17   Now, the task for business is to convince

18   these pragmatists that in particular situations,

19   it's to their benefit for the businesses to combine

20   and use the information that they're putting

21   together about them.

22   My hope is that through workshops like

23   this, we can help bridge the information and trust

24   gaps and enhance public and business awareness of

25   what is and what is not going on out there.

307

1   I'm not going to get into the debate about

2   the value of privacy policies, but I think we can

3   all agree that shedding more light and fresh air on

4   this subject has to be a good thing.

5   Again, I just want to thank all the

6   panelists for contributing to this workshop and to

7   remind you that we do have a record that will

8   remain open for 30 days, and I encourage you to

9   file comments.

10   Thank you very much for coming.

11   (Timed noted: 4:51 p.m.)

12   -   -   -   -   -

13

14

15

16

17

18

19

20

21

22

23

24

25

308

```
 1    C E R T I F I C A T I O N   O F   R E P O R T E R

 2

 3    CASE TITLE:  MERGING AND EXCHANGING CONSUMER DATA

 4    WORKSHOP

 5    MATTER NO.:  P014803

 6    HEARING DATE:  MARCH 13, 2001

 7

 8         We HEREBY CERTIFY that the transcript

 9    contained herein is a full and accurate transcript

10    of the notes taken by us at the hearing on the

11    above cause before the FEDERAL TRADE COMMISSION to

12    the best of our knowledge and belief.

13

14                         DATED: MARCH 26, 2001

15

16                         SALLY J. BOWLING

17

18                         DEBRA L. MAHEUX

19

20    C E R T I F I C A T I O N   O F   P R O O F R E A D E

21         I HEREBY CERTIFY that I proofread the

22    transcript for accuracy in spelling, hyphenation,

23    punctuation and format.

24

25                         DIANE QUADE
```

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025

Exhibit D

Web's Hot New Commodity: Privacy

Giles Sequeira now sells personal details about himself to advertisers.

GARETH PHILLIPS FOR THE WALL STREET JOURNAL

By Julia Angwin and Emily Steel
Updated Feb. 28, 2011 12:01 am ET

As the surreptitious tracking of Internet users becomes more aggressive and widespread, tiny start-ups and technology giants alike are pushing a new product: privacy.

Companies including Microsoft Corp., McAfee Inc.—and even some online-tracking companies themselves—are rolling out new ways to protect users from having their movements monitored online. Some are going further and starting to pay people a commission every time their personal details are used by marketing companies.

"Data is a new form of currency," says Shane Green, chief executive of a Washington start-up, Personal Inc., which has raised $7.6 million for a business that aims to help people profit from providing their personal information to advertisers.

The Wall Street Journal's year-long What They Know investigation into online tracking has exposed a fast-growing network of hundreds of companies that collect highly personal details about Internet users—their online activities, political views, health worries, shopping habits,

financial situations and even, in some cases, their real names—to feed the $26 billion U.S. online-

TO READ THE FULL STORY

SUBSCRIBE

SIGN IN

financial situations and even, in some cases, their real names—to feed the $26 billion U.S. online-

UPCOMING EVENTS

June

12:00 PM - 1:45 PM EDT

WSJ Women In: Intelligent Investing

107

11:00 AM - 5:00 PM EDT

June

24

2021

Global Food Forum

1:00 PM - 1:45 PM EDT

June

30

2021

WSJ Pro Cybersecurity Webinar: Aligning IT and Cybersecurity

ADD TO CALENDAR

Exhibit E

Commissioner Pamela Jones Harbour

Remarks Before FTC Exploring Privacy Roundtable
Washington, D.C
December 7, 2009

Introduction

Welcome back from lunch, and thank you for the opportunity to offer a few thoughts to begin the afternoon.

As many of you know, my time at the FTC is coming to a close. Throughout my term, privacy issues have been among my highest priorities. I am encouraged that the Commission, through this roundtable series, is now engaging stakeholders in a holistic discussion of privacy. The 2007 Ehavioral Town Hall initiated an important conversation by focusing attention on behavioral targeting. But even more importantly, the Town Hall raised the key questions that have since triggered a return to first principles, as the FTC re-evaluates the frameworks it uses to analyze privacy.

More Data = Need for Greater Attention to Privacy

As part of its promise of change, the current Administration has embraced technology and innovation, along with a new era of openness. But real change cannot just be aspirational. It requires concrete action. And unfortunately, with respect to privacy, I believe action has not been a high enough priority to date. I certainly do not intend to criticize Representative Boucher's efforts to craft legislative guidance on behavioral advertising. But as I have previously stated, the United

States needs comprehensive privacy legislation. If we continue the piecemeal approach to privacy in this country, we merely push aside the underlying issues.

The privacy debate goes far beyond online advertising, because behavioral targeting represents just one aspect of a multifaceted privacy conundrum. Data collection, aggregation, and use (as well as reuse, sale and resale) are driving the creation of on- and offline "digital dossiers." Capturing data reflecting individual interests and habits is an enormous and growing business – evidence that consumer privacy is under siege.

Online advertising is an enormous source of information collected about consumers, and serves as an important lens to focus our understanding of data collection and use. Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.

Collection of consumer data is by no means new. Census information, credit reports, and Nielsen data have existed for decades. The Internet, however, enables the creation of vastly larger quantities of consumer data. These data are collected every time we send email, update status on a social networking site, read a news article, run a search, or make an online purchase.

Of course, these technologies have the potential to offer valuable benefits to consumers. The problem, however, is that many consumers are completely unaware of the privacy implications of these services, which makes it difficult for consumers to exercise informed choices about the sites they visit and the data they disclose. In many instances, consumers pay for "free" content and services by disclosing their personal information. Their data are then used to generate targeted advertising that subsidizes online activities.

I am especially troubled by the asymmetry between consumer perceptions and business realities. If consumers do not comprehend how their personal information is collected and used, it is impossible for them to knowingly consent to either disclosure or use. And once data are shared, they cannot simply be recalled or deleted. The cumulative consequences for consumers are magnified, whether they realize it or not.

It is possible that small, discrete disclosures of information do not raise concerns for an individual consumer. But large aggregations of data, based on a lifetime of commercial activity, might evoke a different response. I fear we may reach a "tipping point" whereby consumers decide they want to exercise greater control over the use of their data, but their attempts to exercise control become futile, because so much of their digital life already has been exposed.

Industry attempts to provide notice and choice to consumers have been insufficient thus far. I hope we would all agree that disclosures about information collection, use, and control are not meaningful if they are buried deep within opaque privacy policies. Even if we can decipher the cryptic disclosures, they provide consumers with no meaningful access or choice, which renders those concepts largely illusory. We have strayed far from the Fair Information Practices that should serve as a baseline for any comprehensive privacy legislation.

All of this matters because consumers really do care about their personal privacy, and are willing to take steps to protect it. The findings of the Turow/Hoofnagle report conclude that 66 percent of American adults *reject* tailored ads to begin with. That number increases to over 75 percent when consumers are actually educated about the relevant marketing techniques. Yet, companies are not delivering the privacy protections that consumers prefer.

Even where consumers have the ability to opt-out, the effects are limited. If consumer data are unavailable from one source, often they can be obtained from another. Flash cookies and other

Page 3 of 6

technology largely circumvent cookie controls. We may soon long for the day when all we worried about were cookies. For every company crafting a response that addresses notice, choice, or transparency, there are several more firms trying to parse and evade the intent of Commission guidance. We have entered a digital arms race, and the current outlook is troubling.

<u>Privacy = Consumer Protection + Competition</u>

Privacy issues are important enough that the Commission should use every possible tool at its disposal. During my term as a Commissioner, I have been immersed in both consumer protection and competition issues. I have steadfastly argued that the Commission should apply its competition expertise to the privacy arena.

For example, when the Commission approved the Google/DoubleClick merger in December 2007, I wrote a dissenting statement that, among other things, highlighted the nexus between privacy and competition. While my colleagues at the time disagreed with my premise, subsequent changes in the marketplace have reinforced the validity of my concerns, as well as my premise that privacy protection is increasingly viewed as a non-price dimension of competition.

My dissent in Google/DoubleClick proposed the concept of a market for data itself, separate from markets for the services fueled by the data. The dissent discussed John Battelle's "database of intentions" concept, which he describes as the "aggregate results of every search ever entered, every result list ever tendered, and every path taken as a result." Battelle asserts that no single company controls this collection of information, but posits that a few select companies share control. One of my key concerns in Google/DoubleClick was that the merged entity might move closer to dominating the database of intentions, and that the network effects generated by combining the two firms might have long-term negative consequences for consumers. In response to questions raised

Page 4 of 6

during the concurrent U.S. and EU review of the proposed Google/DoubleClick merger, Google

assured regulators that the deal was not motivated by a desire to enter the behavioral advertising

market. In March of this year, however, the company did in fact begin to engage in interest-based,

or behavioral, advertising.

And last month, Google purchased mobile advertising company AdMob. This acquisition

enhanced Google's ability to extend its advertising strategy into the fast-growing mobile market –

a important market in which I hope, and expect, the Commission will remain vigilant.

Turbulent economic times are forcing companies to seek out new sources of revenue. Those

sources are driven, in turn, by increasingly large amounts of data, as well as the ability to mine the

various connections between pieces of data. As firms continue to develop new data-based markets –

including, for example, cloud computing and smart grid services – we must engage in more serious

inquiries regarding both the privacy and competition issues that affect consumers.

It is worth noting that, to the extent one might define a putative market for consumer data,

recent mergers have further concentrated the competitive landscape. It may also be the case that

Comcast's announced acquisition of NBC from GE should be analyzed from both competition and

consumer protection angles.

In any event, competition on the basis of privacy protection is likely to increase as consumer

awareness grows. The issues raised by data collection and use provide ripe opportunities for

companies to develop pro-consumer privacy tools, and to market these features to distinguish

themselves from competitors.

Conclusion

I know the Commission will continue to be the thought leader on privacy. I will certainly do my part to push the Commission, as I have done for six years now, by challenging mainstream opinions and asking tough questions. Wherever the conversation may lead, I am proud of the efforts of talented Commission staff, and extremely gratified that we have reached the point where we are hosting today's roundtable.

Thank you.

Exhibit F

ECONOMICS & POLICY

Big Data Knows What You're Doing Right Now

By Martha C. White | July 31, 2012

"Big Brother is watching you." That's a line from the dystopian classic *1984*, but it's also far closer to reality than most Americans realize. No, there's not some totalitarian government spy in a trench coat following you, but you are being watched — not by a dictator, but by a handful of companies that make big bucks aggregating tiny scraps of information about you and putting the puzzle pieces together to build your digital profile. Eight lawmakers are demanding that these companies crack open their vaults so Congress can see what they're compiling about us and what they're doing with it.

Getty Images

Right now, this multibillion-dollar industry is largely unregulated. A *New York Times* article earlier this year about a data-mining company prompted the two co-chairs of the Bipartisan Congressional Privacy Caucus and six other Congress members to send a letter to nine companies that collect personal data. They've asked these corporations where they get their data, how they slice and dice it, and to whom they sell and share it.

"By combining data from numerous offline and online sources, data brokers have developed hidden dossiers on almost every U.S. consumer," the letter says. "This large scale aggregation of the personal information of hundreds of millions of American citizens raises a number of serious privacy concerns."

Information is currency, but we tend to forget that. The way we blindly click "okay" on privacy policies, geolocate where we want to eat and play games with our friends on mobile apps to kill time, we're basically putting it all on the table. The explosion of social media and the use of Facebook as a log-in for everything from news sites to online retailers gives data companies a much deeper peek into your personal life and tells them much more about your likes, preferences and habits.

(MORE: Why Smartphones Won't Be Replacing Wallets Anytime Soon)

RELATED

Big Data on Campus *The New York Times*

Companies Suggest Ways Government Data Could Be More Transparent *The Washington Post*

wouldn't think twice about each individual data point, but you can connect the dots," he says. The result is profiling — by ethnicity, by age, by education and income level. The company profiled in the Times' article has literally dozens of profiles of types of people.

And after we give our information away, we have no idea what companies do with it. Unlike credit reporting agencies, which are required to let you see the composite picture of you they've created with the data they mine and organize, data companies keep their vast virtual warehouses under lock and key.

Most of the time, this information is used to sell you stuff. This has the potential to be sneaky — if it knows enough about you, a company can figure out what type of ad is most likely to sway you — but a lot of it isn't inherently bad and might be helpful. If I'm searching for a place to stay in New York City, for instance, and an ad for a hotel pops up on a news site I'm visiting two days later with a discount offer, this could be useful.

(**MORE**: Retailers Embrace Sales on a Smaller Scale)

But that's not what concerns lawmakers and privacy experts. They worry that people's virtual selves could get them written off as undesirable, whether the depiction is correct or not. There's also the question of accuracy in general. Some consumer groups estimate that up to 25% of credit reports have errors, and those errors can lead to difficulty getting a loan or other type of credit. Without any way to look at our consumer profiles, people have no idea what marketers and other interested parties see and how they're judging us.

"Outside the United States, most foreign countries grant a legal right for people to access personal info held by third parties," says Reidenberg. He says this Congressional inquiry is a good start toward establishing some rules about data transparency and disclosure in this country. The letter sent by lawmakers gives the nine companies three weeks to respond. Depending on how forthcoming they are — and they might not be; this committee doesn't have subpoena power — Americans could get a potentially eye-opening look at how corporate America views each of us.

VIDEO: They Know What You Do: Data Mining on the Internet

Exhibit G

GLOBAL EDITION

The New York Times

WITH THE International Herald Tribune

You for Sale: Mapping, and Sharing, the Consumer Genome

By NATASHA SINGER

Published: June 16, 2012

IT knows who you are. It knows where you live. It knows what you do.

t peers deeper into American life than the F.B.I. or the I.R.S., or those prying digital eyes at Facebook and Google. If you are an American adult, the odds are that it knows things like your age, race, sex, weight, height, marital status, education level, politics, buying habits, household health worries, vacation dreams — and on and on.

Right now in Conway, Ark., north of Little Rock, more than 23,000 computer servers are collecting, collating and analyzing consumer data for a company that, unlike Silicon Valley's marquee names, rarely makes headlines. It's called the Acxiom Corporation, and it's the quiet giant of a multibillion-dollar industry known as database marketing.

Few consumers have ever heard of Acxiom. But analysts say it has amassed the world's largest commercial database on consumers — and that it wants to know much, much more. Its servers process more than 50 trillion data "transactions" a year. Company executives have said its database contains information about 500 million active consumers worldwide, with about 1,500 data points per person. That includes a majority of adults in the United States.

Such large-scale data mining and analytics — based on information available in public records, consumer surveys and the like — are perfectly legal. Acxiom's customers have included big banks like Wells Fargo and HSBC, investment services like E*Trade, automakers like Toyota and Ford, department stores like Macy's — just about any major company looking for insight into its customers.

For Acxiom, based in Little Rock, the setup is lucrative. It posted profit of $77.26 million in its latest fiscal year, on sales of $1.13 billion.

But such profits carry a cost for consumers. Federal authorities say current laws may not be equipped to handle the rapid expansion of an industry whose players often collect and sell sensitive financial and health information yet are nearly invisible to the public. In essence, it's as if the ore of our data-driven lives were being mined, refined and sold to the highest bidder, usually without our knowledge — by companies that most people rarely even know exist.

Julie Brill, a member of the Federal Trade Commission, says she would like data brokers in general to tell the public about the data they collect, how they collect it, whom they share it with and how it is used. "If someone is listed as diabetic or pregnant, what is happening with this information? Where is the information going?" she asks. "We need to figure out what the rules should be as a society."

Although Acxiom employs a chief privacy officer, Jennifer Barrett Glasgow, she and other executives declined requests to be interviewed for this article, said Ines Rodriguez Gutzmer, director of corporate communications.

In March, however, Ms. Barrett Glasgow endorsed increased industry openness. "It's not an unreasonable request to have more transparency among data brokers," she said in an interview with The New York Times. In marketing materials, Acxiom promotes itself as "a global thought leader in addressing consumer privacy issues and earning the public trust."

But, in interviews, security experts and consumer advocates paint a portrait of a company with practices that privilege corporate clients' interests over those of consumers and contradict the company's stance on transparency. Acxiom's marketing materials, for example, promote a special security system for clients and associates to encrypt the data they send. Yet cybersecurity experts who examined Acxiom's Web site for The Times found basic security lapses on an online form for consumers seeking access to their own profiles. (Acxiom says it has fixed the broken link that caused the problem.)

In a fast-changing digital economy, Acxiom is developing even more advanced techniques to mine and refine data. It has recruited talent from Microsoft, Google, Amazon.com and Myspace and is using a powerful, multiplatform approach to predicting consumer behavior that could raise its standing among investors and clients.

Of course, digital marketers already customize pitches to users, based on their past activities. Just think of "cookies," bits of computer code placed on browsers to keep track of online activity. But Acxiom, analysts say, is pursuing far more comprehensive techniques in an effort to influence consumer decisions. It is integrating what it knows about our offline, online and even mobile selves, creating in-depth behavior portraits in pixilated detail. Its executives have called this approach a "360-degree view" on consumers.

"There's a lot of players in the digital space trying the same thing," says Mark Zgutowicz, a Piper Jaffray analyst. "But Acxiom's advantage is they have a database of offline information that they have been collecting for 40 years and can leverage that expertise in the digital world."

Yet some prominent privacy advocates worry that such techniques could lead to a new era of consumer profiling.

Jeffrey Chester, executive director of the Center for Digital Democracy, a nonprofit group in Washington, says: "It is Big Brother in Arkansas."

SCOTT HUGHES, an up-and-coming small-business owner and Facebook denizen, is Acxiom's ideal consumer. Indeed, it created him.

Mr. Hughes is a fictional character who appeared in an Acxiom investor presentation in 2010. A frequent shopper, he was designed to show the power of Acxiom's multichannel approach.

In the presentation, he logs on to Facebook and sees that his friend Ella has just become a fan of Bryce Computers, an imaginary electronics retailer and Acxiom client. Ella's update prompts Mr. Hughes to check out Bryce's fan page and do some digital window-shopping for a fast inkjet printer.

Such browsing seems innocuous — hardly data mining. But it cues an Acxiom system designed to recognize consumers, remember their actions, classify their behaviors and influence them with tailored marketing.

When Mr. Hughes follows a link to Bryce's retail site, for example, the system recognizes him from his Facebook activity and shows him a printer to match his interest. He registers on the site, but doesn't buy the printer right away, so the system tracks him online. Lo and behold, the next morning, while he scans baseball news on ESPN.com, an ad for the printer pops up again.

That evening, he returns to the Bryce site where, the presentation says, "he is instantly recognized" as having registered. It then offers a sweeter deal: a $10 rebate and free shipping.

It's not a random offer. Acxiom has its own classification system, PersonicX, which assigns consumers to one of 70 detailed socioeconomic clusters and markets to them accordingly. In this situation, it pegs Mr. Hughes as a "savvy single" — meaning he's in a cluster of mobile, upper-middle-class people who do their banking online, attend pro sports events, are sensitive to prices — and respond to free-shipping offers.

Correctly typecast, Mr. Hughes buys the printer.

But the multichannel system of Acxiom and its online partners is just revving up. Later, it sends him coupons for ink and paper, to be redeemed via his cellphone, and a personalized snail-mail postcard suggesting that he donate his old printer to a nearby school.

Analysts say companies design these sophisticated ecosystems to prompt consumers to volunteer enough personal data — like their names, e-mail addresses and mobile numbers — so that marketers can offer them customized appeals any time, anywhere.

Still, there is a fine line between customization and stalking. While many people welcome the convenience of personalized offers, others may see the surveillance engines behind them as intrusive or even manipulative.

"If you look at it in cold terms, it seems like they are really out to trick the customer," says Dave Frankland, the research director for customer intelligence at Forrester Research. "But they are actually in the business of helping marketers make sure that the right people are getting offers they are interested in and therefore establish a relationship with the company."

DECADES before the Internet as we know it, a businessman named Charles Ward planted the seeds of Acxiom. It was 1969, and Mr. Ward started a data processing company in Conway called Demographics Inc., in part to help the Democratic Party reach voters. In a time when Madison Avenue was deploying one-size-fits-all national ad campaigns, Demographics and its lone computer used public phone books to compile lists for direct mailing of campaign material.

Today, Acxiom maintains its own database on about 190 million individuals and 126 million households in the United States. Separately, it manages customer databases for or works with 47 of the Fortune 100 companies. It also worked with the government after the September 2001 terrorist attacks, providing information about 11 of the 19 hijackers.

To beef up its digital services, Acxiom recently mounted an aggressive hiring campaign. Last July, it named Scott E. Howe, a former corporate vice president for Microsoft's advertising business group, as C.E.O. Last month, it hired Phil Mui, formerly group product manager for Google Analytics, as its chief product and engineering officer.

In interviews, Mr. Howe has laid out a vision of Acxiom as a new-millennium "data refinery" rather than a data miner. That description posits Acxiom as a nimble provider of customer analytics services, able to compete with Facebook and Google, rather than as a stealth engine of consumer espionage.

Still, the more that information brokers mine powerful consumer data, the more they become attractive targets for hackers — and draw scrutiny from consumer advocates.

This year, Advertising Age ranked Epsilon, another database marketing firm, as the biggest advertising agency in the United States, with Acxiom second. Most people know Epsilon, if they know it at all, because it experienced a major security breach last year, exposing the e-mail addresses of millions of customers of Citibank, JPMorgan Chase, Target, Walgreens and others. In 2003, Acxiom had its own security breaches.

But privacy advocates say they are more troubled by data brokers' ranking systems, which classify some people as high-value prospects, to be offered marketing deals and discounts regularly, while dismissing others as low-value — known in industry slang as "waste."

Exclusion from a vacation offer may not matter much, says Pam Dixon, the executive director of the World Privacy Forum, a nonprofit group in San Diego, but if marketing algorithms judge certain people as not worthy of receiving promotions for higher education or health services, they could have a serious impact.

"Over time, that can really turn into a mountain of pathways not offered, not seen and not known about," Ms. Dixon says.

Until now, database marketers operated largely out of the public eye. Unlike consumer reporting agencies that sell sensitive financial information about people for credit or employment purposes, database marketers aren't required by law to show consumers their own reports and allow them to correct errors. That may be about to change. This year, the F.T.C. published a report calling for greater transparency among data brokers and asking Congress to give consumers the right to access information these firms hold about them.

ACXIOM'S Consumer Data Products Catalog offers hundreds of details — called "elements" — that corporate clients can buy about individuals or households, to augment their own marketing databases. Companies can buy data to pinpoint households that are concerned, say, about allergies, diabetes or "senior needs." Also for sale is information on sizes of home loans and household incomes.

Clients generally buy this data because they want to hold on to their best customers or find new ones — or both.

A bank that wants to sell its best customers additional services, for example, might buy details about those customers' social media, Web and mobile habits to identify more efficient ways to market to them. Or, says Mr. Frankland at Forrester, a sporting goods chain whose best customers are 25- to 34-year-old men living near mountains or beaches could buy a list of a million other people with the same characteristics. The retailer could hire Acxiom, he says, to manage a campaign aimed at that new group, testing how factors like consumers' locations or sports preferences affect responses.

But the catalog also offers delicate information that has set off alarm bells among some privacy advocates, who worry about the potential for misuse by third parties that could take aim at vulnerable groups. Such information includes consumers' interests — derived, the catalog says, "from actual purchases and self-reported surveys" — like "Christian families," "Dieting/Weight Loss," "Gaming-Casino," "Money Seekers" and "Smoking/Tobacco." Acxiom also sells data about an individual's race, ethnicity and country of origin. "Our Race model," the catalog says, "provides information on the major racial category: Caucasians, Hispanics, African-Americans, or Asians." Competing companies sell similar data.

Acxiom's data about race or ethnicity is "used for engaging those communities for marketing purposes," said Ms. Barrett Glasgow, the privacy officer, in an e-mail response to questions.

There may be a legitimate commercial need for some businesses, like ethnic restaurants, to know the race or ethnicity of consumers, says Joel R. Reidenberg, a privacy expert and a professor at the Fordham Law School.

"At the same time, this is ethnic profiling," he says. "The people on this list, they are being sold based on their ethnic stereotypes. There is a very strong citizen's right to have a veto over the commodification of their profile."

He says the sale of such data is troubling because race coding may be incorrect. And even if a data broker has correct information, a person may not want to be marketed to based on race.

"DO you really know your customers?" Acxiom asks in marketing materials for its shopper recognition system, a program that uses ZIP codes to help retailers confirm consumers' identities — without asking their permission.

"Simply asking for name and address information poses many challenges: transcription errors, increased checkout time and, worse yet, losing customers who feel that you're invading their privacy," Acxiom's fact sheet explains. In its system, a store clerk need only "capture the shopper's name from a check or third-party credit card at the point of sale and then ask for the shopper's ZIP code or telephone number." With that data Acxiom can identify shoppers within a 10 percent margin of error, it says, enabling stores to reward their best customers with special offers. Other companies offer similar services.

"This is a direct way of circumventing people's concerns about privacy," says Mr. Chester of the Center for Digital Democracy.

Ms. Barrett Glasgow of Acxiom says that its program is a "standard practice" among retailers, but that the company encourages its clients to report consumers who wish to opt out.

Acxiom has positioned itself as an industry leader in data privacy, but some of its practices seem to undermine that image. It created the position of chief privacy officer in 1991, well ahead of its rivals. It even offers an online request form, promoted as an easy way for consumers to access information Acxiom collects about them.

But the process turned out to be not so user-friendly for a reporter for The Times.

In early May, the reporter decided to request her record from Acxiom, as any consumer might. Before submitting a Social Security number and other personal information, however, she asked for advice from a cybersecurity expert at The Times. The expert examined Acxiom's Web site and immediately noticed that the online form did not employ a standard encryption protocol — called https — used by sites like Amazon and American Express. When the expert tested the form, using software that captures data sent over the Web, he could clearly see that the sample Social Security number he had submitted had not been encrypted. At that point, the reporter was advised not to request her file, given the risk that the process might expose her personal information.

Later in May, Ashkan Soltani, an independent security researcher and former technologist in identity protection at the F.T.C., also examined Acxiom's site and came to the same conclusion. "Parts of the site for corporate clients are encrypted," he says. "But

for consumers, who this information is about and who stand the most to lose from data collection, they don't provide security."

Ms. Barrett Glasgow says that the form has always been encrypted with https but that on May 11, its security monitoring system detected a "broken redirect link" that allowed unencrypted access. Since then, she says, Acxiom has fixed the link and determined that no unauthorized person had gained access to information sent using the form.

On May 25, the reporter submitted an online request to Acxiom for her file, along with a personal check, sent by Express Mail, for the $5 processing fee. Three weeks later, no response had arrived.

Regulators at the F.T.C. declined to comment on the practices of individual companies. But Jon Leibowitz, the commission chairman, said consumers should have the right to see and correct personal details about them collected and sold by data aggregators.

After all, he said, "they are the unseen cyberazzi who collect information on all of us."

A version of this article appeared in print on June 17, 2012, on page BU1 of the New York edition with the headline: You For Sale.

Exhibit H

United States Senate

COMMITTEE ON COMMERCE, SCIENCE,
AND TRANSPORTATION

WASHINGTON, DC 20510–6125

WEB SITE: http://commerce.senate.gov

October 9, 2012

Mr. Scott E. Howe
President and Chief Executive Officer
Acxiom
601 East 3rd Street
Little Rock, Arkansas 72201

Dear Mr. Howe,

I am writing to request information about your company's data collection and use practices. For years, companies like yours, commonly referred to as "data brokers," have collected data about consumers and then sold that information to interested parties for a variety of purposes.

Because consumers are now able to conduct nearly all of their daily business online, an unprecedented amount of personal, medical, and financial information about them can be mined, collected, and sold. Consumers will increasingly use the Internet to make purchases, plan trips, research medical conditions, interact with friends and relatives, do their jobs, and pursue their interests. An ever-increasing percentage of their lives will be available for download and the digital footprint they will inevitably leave behind will become more specific and potentially damaging, if used improperly.

As use of the Internet has grown, the data broker industry has already evolved to take advantage of the increasingly specific pieces of information about consumers that are now available. While companies like yours engage in these practices, consumers are largely unaware of how your company uses their sensitive information for financial gain.[1]

In recent years, your industry's practices have generated scrutiny from various entities, including major media outlets and the Federal Trade Commission. In March, the FTC released a report on privacy, where it advocated for targeted legislation to "address the invisibility of, and consumers' lack of control over, data brokers' collection and use of consumer information." In making its recommendation, the FTC noted that "efforts of the data broker industry to establish self-regulatory rules concerning consumer privacy have fallen short."[2]

---

[1] *You for Sale: Mapping, and Sharing the Consumer Genome,* The New York Times (June 16, 2012).

[2] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers* (March 2012).

Letter to Mr. Howe
October 9, 2012

Companies in your industry have also in recent years suffered several high-profile data breaches.[3] Through these breaches, computer hackers obtained sensitive consumer data that had been collected and stored by companies in your industry. These breaches highlighted the need for both the Congress and the American people to better understand what consumer information is being collected and stored. The breaches served as a stark reminder that very little is known about the information companies likes yours have about American consumers.

Since I became Chairman of the Senate Commerce Committee, I have sought to better understand your industry. Because your industry has monetized consumer data, it is critical that we understand what information companies like yours are already collecting and selling. Yet, answers to basic questions remain elusive. These questions include:

- What data about consumers does your industry collect?

- How specific is this data?

- How does your industry obtain this data?

- Who buys this data and how is it used?

To answer these questions and help the Committee better understand your company's practices, I ask that you provide responses to the following requests by Friday, November 2, 2012. In each of the requests below, "company," "you," or "your" refers to Acxiom and any of its parents, subsidiaries, and affiliates. "Company" includes trade names, operations under assumed names, fictitious business names, corporations, limited liability companies, unincorporated divisions, joint ventures, partnerships, sole proprietorships, associations, cooperatives, and any other legal entities.

1. Provide a list identifying each entity, including private sources and government agencies and offices, from which you have collected or otherwise received data from or about consumers at any time since January 1, 2009, and list each type of data you have collected or otherwise received from each entity. For each entity listed, provide the contract between your company and the entity, which includes the terms related to the transfer of consumer data and the amount of money your company has paid that entity to acquire consumer data since January 1, 2009.

2. Describe each method or mechanism you have used to collect data from or about consumers at any time since January 1, 2009, including the method or mechanism used by entities that have provided data to your company. For each data collection method or mechanism, please indicate whether and how the collected data is linked to specific consumers, computers, or devices.

---

[3] *Breach Brings Scrutiny*, The Wall Street Journal (April 5, 2011); *United States v. ChoicePoint, Inc.*, No. 1 06-CV-0198 (N.D. Ga. filed Jan. 30, 2006); *In re Reed Elsevier Inc. & Seisint, Inc.*, FTC Docket No. C-4226 (July 29, 2008).

Letter to Mr. Howe
October 9, 2012

3. Identify the consumer data your company has collected, received, or otherwise obtained since January 1, 2009, including documents sufficient to show the specificity of that consumer data.

4. List each product or service you have offered to third parties at any time since January 1, 2009, that uses, incorporates, or otherwise relies on data from or about consumers. For each product or service, please describe:

    a. Each type of data that may be used to develop or otherwise provide the product or service;
    b. Each type of data that you offer or otherwise provide to a third party using the product or service;
    c. Each type of entity or individual to which you sell, provide, or otherwise give access to the product or service;
    d. Any prohibitions, restrictions, or limitations on the sale or use of, or access to, the product or service;
    e. Whether or not the product or service is subject to the Fair Credit Reporting Act (FCRA) and, if so, each step you take to ensure compliance with all relevant provisions of the FCRA; and
    f. Whether consumers can opt-out of having their data included in the product or service, and, if so:
        i.   Describe the process through which a consumer can opt out, including any fee a consumer must pay to exercise their opt-out rights, and provide screen shots or documents setting forth each step a consumer must take to exercise the opt out.
        ii. Describe and provide documents demonstrating how you make consumers aware of their opt-out rights.
        iii. Since January 1, 2009, provide the number of consumers that have opted out.

5. For each product or service identified in response to request 4, please provide:

    a. Copies of all advertising or marketing materials regarding the product or service;
    b. Screen shots or other documents setting forth each step an entity must take to access, implement, and use the product or service; and
    c. Representative samples of all reports, lists, or other documents that may be created or developed by a third party using the product or service.

6. Identify any entity or individual that your company sold, provided, or otherwise gave access to each of the products or services identified in response to request 4 since January 1, 2009. For each entity or individual listed, please provide the following:

    a. Documents sufficient to show the type of data that you sold or otherwise provided to the entity or individual, including each type of data that was sold or provided and the specificity of the consumer data that was shared;
    b. The amount of money the entity or individual paid for the data;
    c. The individual's or entity's stated, contractual, or intended use of the data;

Letter to Mr. Howe
October 9, 2012

      d. Contracts or agreements between your company and the entity or individual; and

      e. The manner in which your company provided access to the data, and any conditions, limitations, or restrictions under which you provide the data to the entity or individual.

7. Describe any processes, including audits, your company employs to determine whether a third party may access each product or service identified in response to request 4 and provide:

      a. Copies of all application, registration, or approval forms or other documents that your company requires prior to granting a third party access to the product or service;

      b. Documents or materials your company uses to verify, vet, or otherwise approve access by the third party; and

      c. The total number of instances where your company has refused to provide access to the product or service and, for each such instance, describe and provide documents regarding the reason(s) your company refused to provide access.

8. Do you provide consumers notice about your data collection, use, or sharing practices? If yes, please describe how you provide notice and provide copies of each notice.

9. Can consumers access, correct, delete, or suppress the information you maintain about them? If not, why not? If yes:

      a. List each type of data consumers can access, correct, delete, or suppress and each type of data consumers cannot access, correct, delete, or suppress;

      b. Describe the process through which a consumer can access, correct, delete, or suppress the data, including any fee a consumer must pay to exercise their rights, and provide screen shots or documents setting forth each step a consumer must take to access, correct, delete, or suppress the information maintained about them;

      c. Describe and provide documents demonstrating how you make consumers aware of their access, correction, deletion, or suppression rights; and

      d. Since January 1, 2009, provide the number of consumers that have requested access, corrections, deletions, or suppressions and the number of consumers that have received access, corrections, deletions, or suppressions. In each instance where you have not granted a consumer's request to access, correct, delete, or suppress the information you maintain about them, describe the reason(s) for the refusal and provide all relevant documents and correspondence.

10. Provide communications you have received from consumers or other entities, including the Better Business Bureau or state agencies, regarding the accuracy of the information you collect or maintain about consumers, or consumers' ability to access, correct, suppress, delete, or otherwise opt out of the collection, use, or sharing of the information you collect, use, or maintain about consumers.

11. To the extent not already provided, please provide copies of each claim or disclosure you make to consumers regarding: your data collection and use practices; each product or
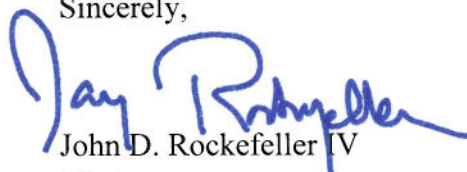
Letter to Mr. Howe
October 9, 2012

service that uses or otherwise relies on data from or about consumers; the accuracy of the data you maintain about them; and their ability to access, correct, delete, suppress or otherwise opt out of the collection, use, or sharing of the information collected, used, or maintained about them.

12. Provide copies of all articles of incorporation, annual or other periodic reports, and audited financial statements, including any accompanying notes and management discussion and analysis, for your company for the past 5 years.

The Committee is conducting this investigation under the authority of Senate Rules XXV and XXVI. An attachment to this letter provides additional information about how to respond to the Committee's request. If you have any questions, please contact Melanie Tiano or Erik Jones with the Committee staff at (202) 224-1300.

Sincerely,

John D. Rockefeller IV
Chairman

Enclosure

cc: Kay Bailey Hutchison
        Ranking Member

Exhibit I

ED MARKEY
UNITED STATES SENATOR FOR MASSACHUSETTS

JULY 24, 2012

BIPARTISAN GROUP OF LAWMAKERS QUERY DATA BROKERS ABOUT PRACTICES INVOLVING CONSUMERS' PERSONAL INFORMATION

Multi-billion dollar industry practices may have long-term impact on access to education, health care, employment

WASHINGTON, D.C. – A bipartisan group of six lawmakers joined Reps. Edward J. Markey (D-Mass.) and Joe Barton (R-Texas), co-Chairmen of the Congressional Bi-Partisan Privacy Caucus, in letters sent today to nine major data brokerage companies querying each about how it collects, assembles and sells consumer information to third parties. Other signatories on the letters include Reps. Henry A. Waxman (D-Calif.), Steve Chabot (R-Ohio), G.K. Butterfield (D-N.C.), Austin Scott (R-Ga.), Bobby Rush (D-Ill.), and Jan Schakowsky (D-Ill.).

Representing a multi-billion dollar industry, data brokers have aggregated information about hundreds of millions of Americans from both online and offline sources, which they then sell to third parties for targeted advertising and other purposes, often with little consumer knowledge. A recent New York Times story, "A Data Giant is Mapping, and Sharing, the Consumer Genome" detailed how data brokers have developed consumer profiles that go beyond basic demographic information to include buying habits, household health concerns, political affiliations and even time spent on vacation. The lawmakers' letters request information from the data brokers on polices and practices related to privacy, transparency and consumer notification, including as they relate to children and teens.

"By combining data from numerous offline and online sources, data brokers have developed hidden dossiers on almost every U.S. consumer," write the lawmakers in the letter to the data brokers. **"This large scale aggregation of the personal information of hundreds of millions of American citizens raises a number of serious privacy concerns."**

A copy of the letters to the data brokers can be found HERE.

The companies sent letters include Acxiom, Epsilon (Alliance Data Systems), Equifax, Experian, Harte-Hanks, Intelius, Fair Isaac, Merkle, and Meredith Corp.

The lawmakers ask the nine data brokers to provide information that includes:

- A list of entities that have provided data from or about consumers to the company
- A list of data items collected from or about consumers, and the methods by which it is collected
- Products or services offered to third parties that utilize consumer data.
- The information consumers are given access to, if it is requested, and any policies around sharing or deletion of that data
- Encryption or other safety protocols used to protect data.

###

🖨 PRINT   ✉ EMAIL   👍 LIKE   👍 TWEET

Tags: Privacy, Telecommunications, the Internet & Privacy

PREVIOUS ARTICLE   NEXT ARTICLE

Exhibit J

FEDERAL TRADE COMMISSION

Consumer Information

consumer.ftc.gov

Fake Prize, Sweepstakes, and Lottery Scams

You get a call, email, or letter saying you won a sweepstakes, lottery, or prize — like an iPad, a new car, or something else. But you can tell it's a scam because of what they do next: they ask you to pay money or give them your account information to get the prize. If you pay, you'll lose your money and find out there is no prize.

- 3 Signs of a Prize Scam (#three signs)
- How Scammers Try To Trick You (#how)
- What To Know About Real Contests and Prizes (#what)
- What To Do if You Paid a Scammer (#what to do)
- Report Prize Winnings and Lottery Scams (#report)

3 Signs of a Prize Scam

Who doesn't dream of winning a lot of money or a big prize? That's why scammers still use the promise of a prize to get your money or personal information. The good news is that there are ways to tell you're dealing with a scam.

Here are three signs of a prize scam:

1. **You have to pay to get your prize**. But real prizes are free. So if someone tells you to pay a fee for "taxes," "shipping and handling charges," or "processing fees" to get your prize, you're dealing with a scammer. And if they ask you to pay by wiring money, sending cash, or paying with gift cards or cryptocurrency to get your prize, don't do it. Scammers use these payments because it's hard to track who the money went to. And it's almost impossible to get your money back.

2. **They say paying increases your odds of winning**. But real sweepstakes are free and winning is by chance. It's illegal for someone to ask you to pay to increase your odds of winning. Only a scammer will do that.

3. **You have to give your financial information.** There's absolutely no reason to ever give your bank account or credit card number to claim any prize or sweepstakes. If they ask for this

information, don't give it. It's a scam.

How Scammers Try To Trick You

Scammers will say anything to get your money. Here are ways they try to trick you into thinking you really won a prize.

- **Scammers say they're from the government when they're not.** Scammers try to look official. They want you to think you've won a government-supervised lottery or sweepstakes. They make up fake names like the "National Sweepstakes Bureau," or pretend they're from a real agency (http://www.consumer.ftc.gov/articles/0048-government-imposter-scams) like the Federal Trade Commission. The truth is, the government won't call you to demand money so you can collect a prize.

- **Scammers use names of organizations you might recognize.** Scammers might pretend to be from well-known companies that run real sweepstakes. But no real sweepstakes company will contact you to ask for money so you can claim a prize. If you're unsure, contact the real company directly to find out the truth. And look up the real company's contact information yourself. Don't rely on the person who reached out to you to provide you with the real contact information.

- **Scammers send you a message (via text, email, or social media) to get your personal information.** You might be told that you won a gift card or a discount code to a local store. Or the message may say you won something expensive, like an iPad or a new car from your local dealership. Scammers hope you'll respond with your personal information or click on links that can take your personal information or download malware onto your device. Don't respond.

- **Scammers make it seem like you're the only person who won a prize. But the same text, email, or letter went to lots of people.** If your message came by mail, check the postmark on the envelope or postcard. If your "notice" was mailed by bulk rate, it means many other people got the same notice, too. For other types of messages, check online to see if others are reporting that they got the same message.

- **Scammers say you've won a foreign lottery, or that you can buy tickets for one.** Messages about a foreign lottery are almost certainly from a scammer — and it's a bad idea to respond. First, it's illegal for U.S. citizens to play a foreign lottery, so don't trust someone who asks you to break the law. Second, if you buy a foreign lottery ticket, expect many more offers for fake lotteries or scammy investment "opportunities." Finally, there are no secret systems for winning foreign lotteries, so don't believe someone who tells you they can help you win.

- **Scammers pressure you to act now to get a prize. Scammers want you to hurry up and pay or give them information.** They tell you it's a limited time offer or you have to "act now" to claim your prize. They don't want you to have time to evaluate what's really happening. Don't be rushed — especially if they want you to do something to get your prize.

- **Scammers send you a check and ask you to send some of the money back.** This is a fake check scam. If you deposit the check, it can take the bank weeks to figure out that it's fake. In the meantime, the bank has to make the funds available, so it can look like the money is in your account. But once the bank finds out the check is fake, they'll want you to pay back the funds. Read How to Spot, Avoid, and

Report Fake Check Scams (http://www.consumer.ftc.gov/articles/how-spot-avoid-and-report-fake-check-scams) for more tips.

If you're not sure about a contest or the company sending you a prize notification, search online to see if you find anything about them. Type the name with terms like "review," "complaint," or "scam."

What To Know About Real Contests and Prizes

Plenty of contests are run by reputable marketers and non-profit organizations. But there are some things to know before you drop in a quick entry or follow instructions to claim a prize.

- **Real sweepstakes are free and by chance**. It's illegal to ask you to pay or buy something to enter, or to increase your odds of winning.

- **Contest promoters might sell your information to advertisers**. If you sign up for a contest or a drawing, you're likely to get more promotional mail, telemarketing calls, or spam.

- **Contest promoters have to tell you certain things.** If they call you, the law says they have to tell you that entering is free, what the prizes are and their value, the odds of winning, and how you'd redeem a prize.

- **Sweepstakes mailings must say you don't have to pay to participate.** They also can't claim you're a winner unless you've actually won a prize. And if they include a fake check in their mailing, it has to clearly say that it's non-negotiable and has no cash value.

A special note about skills contests. A skills contest — where you do things like solve problems or answer questions correctly to earn prizes — **can ask you to pay to play**. But you might end up paying repeatedly, with each round getting more difficult and expensive, before you realize it's impossible to win or just a scam. Skills contests can leave contestants with nothing to show for their money and effort.

What To Do if You Paid a Scammer

Scammers often ask you to pay in ways that make it tough to get your money back. No matter how you paid a scammer, the sooner you act, the better. Learn more about how to get your money back (https://www.consumer.ftc.gov/articles/what-do-if-you-were-scammed#Paid).

Report Prize Winnings and Lottery Scams

If you think you've been targeted by a prize scam:

- Report it to the FTC at ReportFraud.ftc.gov (http://reportfraud.ftc.gov)
- You also can contact your state attorney general (https://www.consumerresources.org/file-a-complaint/) and your local consumer protection office

(http://www.usa.gov/directory/stateconsumer/index.shtml).

- If the prize promotion came in the mail, report it to the US. Postal Inspection Service. (http://www.uspis.gov/report/)

- If you think you gave your personal information to a scammer, go to IdentityTheft.gov (http://identitytheft.gov) for steps you can take to protect your identity.

- Tell your friends and family. You could help them avoid getting scammed.

May 2021

Exhibit K

The New York Times | https://www.nytimes.com/2007/05/20/business/20tele.html

Bilking the Elderly, With a Corporate Assist

Richard Guthrie, 92, was tricked into giving banking data to telephone callers, who then stole money from his account, investigators say.
Ozier Muhammad/The New York Times

By Charles Duhigg

May 20, 2007

The thieves operated from small offices in Toronto and hangar-size rooms in India. Every night, working from lists of names and phone numbers, they called World War II veterans, retired schoolteachers and thousands of other elderly Americans and posed as government and insurance workers updating their files.

Then, the criminals emptied their victims' bank accounts.

Richard Guthrie, a 92-year-old Army veteran, was one of those victims. He ended up on scam artists' lists because his name, like millions of others, was sold by large companies to telemarketing criminals, who then turned to major banks to steal his life's savings.

Mr. Guthrie, who lives in Iowa, had entered a few sweepstakes that caused his name to appear in a database advertised by infoUSA, one of the largest compilers of consumer information. InfoUSA sold his name, and data on scores of other elderly Americans, to known lawbreakers, regulators say.

InfoUSA advertised lists of "Elderly Opportunity Seekers," 3.3 million older people "looking for ways to make money," and "Suffering Seniors," 4.7 million people with cancer or Alzheimer's disease. "Oldies but Goodies" contained 500,000 gamblers over 55 years old, for 8.5 cents apiece. One list said: "These people are gullible. They want to believe that their luck can change."

As Mr. Guthrie sat home alone — surrounded by his Purple Heart medal, photos of eight children and mementos of a wife who was buried nine years earlier — the telephone rang day and night. After criminals tricked him into revealing his banking information, they went to Wachovia, the nation's fourth-largest bank, and raided his account, according to banking records.

"I loved getting those calls," Mr. Guthrie said in an interview. "Since my wife passed away, I don't have many people to talk with. I didn't even know they were stealing from me until everything was gone."

Telemarketing fraud, once limited to small-time thieves, has become a global criminal enterprise preying upon millions of elderly and other Americans every year, authorities say. Vast databases of names and personal information, sold to thieves by large publicly traded companies, have put almost anyone within reach of fraudulent telemarketers. And major banks have made it possible for criminals to dip into victims' accounts without their authorization, according to court records.

The banks and companies that sell such services often confront evidence that they are used for fraud, according to thousands of banking documents, court filings and e-mail messages reviewed by The New York Times.

Although some companies, including Wachovia, have made refunds to victims who have complained, neither that bank nor infoUSA stopped working with criminals even after executives were warned that they were aiding continuing crimes, according to government investigators. Instead, those companies collected millions of dollars in fees from scam artists. (Neither company has been formally accused of wrongdoing by the authorities.)

"Only one kind of customer wants to buy lists of seniors interested in lotteries and sweepstakes: criminals," said Sgt. Yves Leblanc of the Royal Canadian Mounted Police. "If someone advertises a list by saying it contains gullible or elderly people, it's like putting out a sign saying 'Thieves welcome here.'"

In recent years, despite the creation of a national "do not call" registry, the legitimate telemarketing industry has grown, according to the Direct Marketing Association. Callers pitching insurance plans, subscriptions and precooked meals collected more than $177 billion in 2006, an increase of $4.5 billion since the federal do-not-call restrictions were put in place three years ago.

That growth can be partly attributed to the industry's renewed focus on the elderly. Older Americans are perfect telemarketing customers, analysts say, because they are often at home, rely on delivery services, and are lonely for the companionship that telephone callers provide. Some researchers estimate that the elderly account for 30 percent of telemarketing sales — another example of how companies and investors are profiting from the growing numbers of Americans in their final years.

While many telemarketing pitches are for legitimate products, the number of scams aimed at older Americans is on the rise, the authorities say. In 2003, the Federal Trade Commission estimated that 11 percent of Americans over age 55 had been victims of consumer fraud. The following year, the Federal Bureau of Investigation shut down one telemarketing ring that stole more than $1 billion, spanned seven countries and resulted in 565 arrests. Since the start of last year, federal agencies have filed lawsuits or injunctions against at least 68 telemarketing companies and individuals accused of stealing more than $622 million.

"Most people have no idea how widespread and sophisticated telemarketing fraud has become," said James Davis, a Federal Trade Commission lawyer. "It shocks even us."

Many of the victims are people like Mr. Guthrie, whose name was among the millions that infoUSA sold to companies under investigation for fraud, according to regulators. Scam artists stole more than $100,000 from Mr. Guthrie, his family says. How they took much of it is unclear, because Mr. Guthrie's memory is faulty and many financial records are incomplete.

What is certain is that a large sum was withdrawn from his account by thieves relying on Wachovia and other banks, according to banking and court records. Though 20 percent of the total amount stolen was recovered, investigators say the rest has gone to schemes too complicated to untangle.

Senior executives at infoUSA were contacted by telephone and e-mail messages at least 30 times. They did not respond.

Wachovia, in a statement, said that it had honored all requests for refunds and that it was cooperating with authorities.

Mr. Guthrie, however, says that thieves should have been prevented from getting access to his funds in the first place.

"I can't understand why they were allowed inside my account," said Mr. Guthrie, who lives near Des Moines. "I just chatted with this woman for a few minutes, and the next thing I knew, they took everything I had."

Sweepstakes a Common Tactic

Investigators suspect that Mr. Guthrie's name first appeared on a list used by scam artists around 2002, after he filled out a few contest entries that asked about his buying habits and other personal information.

He had lived alone since his wife died. Five of his eight children had moved away from the farm. Mr. Guthrie survived on roughly $800 that he received from Social Security each month. Because painful arthritis kept him home, he spent many mornings organizing the mail, filling out sweepstakes entries and listening to big-band albums as he chatted with telemarketers.

"I really enjoyed those calls," Mr. Guthrie said. "One gal in particular loved to hear stories about when I was younger."

Some of those entries and calls, however, were intended solely to create databases of information on millions of elderly Americans. Many sweepstakes were fakes, investigators say, and existed only to ask entrants about shopping habits, religion or other personal details. Databases of such responses can be profitably sold, often via electronic download, through list brokers like Walter Karl Inc., a division of infoUSA.

The list brokering industry has existed for decades, primarily serving legitimate customers like magazine and catalog companies. InfoUSA, one of the nation's largest list brokers and a publicly held company, matches buyers and sellers of data. The company maintains records on 210 million Americans, according to its Web site. In 2006, it collected more than $430 million from clients like Reader's Digest, Publishers Clearinghouse and Condé Nast.

But infoUSA has also helped sell lists to companies that were under investigation or had been prosecuted for fraud, according to records collected by the Iowa attorney general. Those records stemmed from a now completed investigation of a suspected telemarketing criminal.

By 2004, Mr. Guthrie's name was part of a list titled "Astroluck," which included 19,000 other sweepstakes players, Iowa's records show. InfoUSA sold the Astroluck list dozens of times, to companies including HMS Direct, which Canadian authorities had sued the previous year for deceptive mailings; Westport Enterprises, the subject of consumer complaints in Kansas, Connecticut and Missouri; and Arlimbow, a European company that Swiss authorities were prosecuting at the time for a lottery scam.

(In 2005, HMS's director was found not guilty on a technicality. Arlimbow was shut down in 2004. Those companies did not return phone calls. Westport Enterprises said it has resolved all complaints, complies with all laws and engages only in direct-mail solicitations.)

Records also indicate that infoUSA sold thousands of other elderly Americans' names to Windfall Investments after the F.B.I. had accused the company in 2002 of stealing $600,000 from a California woman.

Between 2001 and 2004, infoUSA also sold lists to World Marketing Service, a company that a judge shut down in 2003 for running a lottery scam; to Atlas Marketing, which a court closed in 2006 for selling $86 million of bogus business opportunities; and to Emerald Marketing Enterprises, a Canadian firm that was investigated multiple times but never charged with wrongdoing.

The investigation of Windfall Investments was closed after its owners could not be located. Representatives of Windfall Investments, World Marketing Services, Atlas Marketing and Emerald Marketing Enterprises could not be located or did not return calls.

Steve St. Clair, an Iowa assistant attorney general, investigated the sale of mailing lists that may have been used in the first step of a scam aimed at the elderly.
Ozier Muhammad/The New York Times

The Federal Trade Commission's rules prohibit list brokers from selling to companies engaged in obvious frauds. In 2004, the agency fined three brokers accused of knowingly, or purposely ignoring, that clients were breaking the law. The Direct Marketing Association, which infoUSA belongs to, requires brokers to screen buyers for suspicious activity.

But internal infoUSA e-mail messages indicate that employees did not abide by those standards. In 2003, two infoUSA employees traded e-mail messages discussing the fact that Nevada authorities were seeking Richard Panas, a frequent infoUSA client, in connection with a lottery scam.

"This kind of behavior does not surprise me, but it adds to my concerns about doing business with these people," an infoUSA executive wrote to colleagues. Yet, over the next 10 months, infoUSA sold Mr. Panas an additional 155,000 names, even after he pleaded guilty to criminal charges in Nevada and was barred from operating in Iowa.

Mr. Panas did not return calls.

"Red flags should have been waving," said Steve St. Clair, an Iowa assistant attorney general who oversaw the infoUSA investigation. "But the attitude of these list brokers is that it's not their responsibility if someone else breaks the law."

Millions of Americans Are Called

Within months of the sale of the Astroluck list, groups of scam artists in Canada, the Caribbean and elsewhere had the names of Mr. Guthrie and millions of other Americans, authorities say. Such countries are popular among con artists because they are outside the jurisdiction of the United States.

The thieves would call and pose as government workers or pharmacy employees. They would contend that the Social Security Administration's computers had crashed, or prescription records were incomplete. Payments and pills would be delayed, they warned, unless the older Americans provided their banking information.

Many people hung up. But Mr. Guthrie and hundreds of others gave the callers whatever they asked.

"I was afraid if I didn't give her my bank information, I wouldn't have money for my heart medicine," Mr. Guthrie said.

Criminals can use such banking data to create unsigned checks that withdraw funds from victims' accounts. Such checks, once widely used by gyms and other businesses that collect monthly fees, are allowed under a provision of the banking code. The difficult part is finding a bank willing to accept them.

In the case of Mr. Guthrie, criminals turned to Wachovia.

Between 2003 and 2005, scam artists submitted at least seven unsigned checks to Wachovia that withdrew funds from Mr. Guthrie's account, according to banking records. Wachovia accepted those checks and forwarded them to Mr. Guthrie's bank in Iowa, which in turn sent back $1,603 for distribution to the checks' creators that submitted them.

Within days, however, Mr. Guthrie's bank, a branch of Wells Fargo, became concerned and told Wachovia that the checks had not been authorized. At Wells Fargo's request, Wachovia returned the funds. But it failed to investigate whether Wachovia's accounts were being used by criminals, according to prosecutors who studied the transactions.

In all, Wachovia accepted $142 million of unsigned checks from companies that made unauthorized withdrawals from thousands of accounts, federal prosecutors say. Wachovia collected millions of dollars in fees from those companies, even as it failed to act on warnings, according to records.

In 2006, after account holders at Citizens Bank were victimized by the same thieves that singled out Mr. Guthrie, an executive wrote to Wachovia that "the purpose of this message is to put your bank on notice of this situation and to ask for your assistance in trying to shut down this scam."

But Wachovia, which declined to comment on that communication, did not shut down the accounts.

Banking rules required Wachovia to periodically screen companies submitting unsigned checks. Yet there is little evidence Wachovia screened most of the firms that profited from the withdrawals.

In a lawsuit filed last year, the United States attorney in Philadelphia said Wachovia received thousands of warnings that it was processing fraudulent checks, but ignored them. That suit, against the company that printed those unsigned checks, Payment Processing Center, or P.P.C., did not name Wachovia as a defendant, though at least one victim has filed a pending lawsuit against the bank.

During 2005, according to the United States attorney's lawsuit, 59 percent of the unsigned checks that Wachovia accepted from P.P.C. and forwarded to other banks were ultimately refused by other financial institutions. Wachovia was informed each time a check was returned.

"When between 50 and 60 percent of transactions are returned, that tells you at gut level that something's not right," said the United States attorney in Philadelphia, Patrick L. Meehan.

AFTERMATH Tony Unspach takes care of bills and banking for his grandfather, Richard Guthrie, a victim of fake telemarketers.
Ozier Muhammad/The New York Times

Other banks, when confronted with similar evidence, have closed questionable accounts. But Wachovia continued accepting unsigned checks printed by P.P.C. until the government filed suit in 2006.

Wachovia declined to respond to the accusations in the lawsuit, citing the continuing civil litigation.

Although Wachovia is the largest bank that processed transactions that stole from Mr. Guthrie, at least five other banks accepted 31 unsigned checks that withdrew $9,228 from his account. Nearly every time, Mr. Guthrie's bank told those financial institutions the checks were fraudulent, and his money was refunded. But few investigated further.

The suit against P.P.C. ended in February. A court-appointed receiver will liquidate the firm and make refunds to consumers. P.P.C.'s owners admitted no wrongdoing.

Wachovia was asked in detail about its relationship with P.P.C., the withdrawals from Mr. Guthrie's account and the accusations in the United States attorney's lawsuit. The company declined to comment, except to say: "Wachovia works diligently to detect and end fraudulent use of its accounts. During the time P.P.C. was a customer, Wachovia honored all requests for returns related to the P.P.C. accounts, which in turn protected consumers from loss."

Prosecutors argue that many elderly accountholders never realized Wachovia had processed checks that withdrew from their accounts, and so never requested refunds. Wachovia declined to respond.

The bank's statement continued: "Wachovia is cooperating fully with authorities on this matter."

Some Afraid to Seek Help

By 2005, Mr. Guthrie was in dire straits. When tellers at his bank noticed suspicious transactions, they helped him request refunds. But dozens of unauthorized withdrawals slipped through. Sometimes, he went to the grocery store and discovered that he could not buy food because his account was empty. He didn't know why. And he was afraid to seek help.

"I didn't want to say anything that would cause my kids to take over my accounts," he said. Such concerns play into thieves' plans, investigators say.

"Criminals focus on the elderly because they know authorities will blame the victims or seniors will worry about their kids throwing them into nursing homes," said C. Steven Baker, a lawyer with the Federal Trade Commission. "Frequently, the victims are too distracted from dementia or Alzheimer's to figure out something's wrong."

Within a few months, Mr. Guthrie's children noticed that he was skipping meals and was behind on bills. By then, all of his savings — including the proceeds of selling his farm and money set aside to send great-grandchildren to college — was gone.

State regulators have tried to protect victims like Mr. Guthrie. In 2005, attorneys general of 35 states urged the Federal Reserve to end the unsigned check system.

"Such drafts should be eliminated in favor of electronic funds transfers that can serve the same payment function" but are less susceptible to manipulation, they wrote.

But the Federal Reserve disagreed. It changed its rules to place greater responsibility on banks that first accept unsigned checks, but has permitted their continued use.

Today, just as he feared, Mr. Guthrie's financial freedom is gone. He gets a weekly $50 allowance to buy food and gasoline. His children now own his home, and his grandson controls his bank account. He must ask permission for large or unusual purchases.

And because he can't buy anything, many telemarketers have stopped calling.

"It's lonelier now," he said at his kitchen table, which is crowded with mail. "I really enjoy when those salespeople call. But when I tell them I can't buy anything now, they hang up. I miss the good chats we used to have."

Exhibit L

Prepared Statement of
The Federal Trade Commission on

"Fraud Against Seniors"

Before the

Special Committee on Aging
United States Senate
Indianapolis, Indiana

August 10, 2000

I am Rolando Berrelez, Assistant Regional Director of the Midwest Region of the Federal Trade Commission. I am pleased to appear before you today to present information about the Commission's activities with regard to fraudulent marketing practices, especially those that affect the elderly.[1] The Federal Trade Commission is the primary federal consumer protection agency, with wide-ranging responsibilities over nearly all segments of the economy. In pursuing its mandate of protecting consumers, the Commission enforces the Federal Trade Commission Act,[2] which broadly prohibits unfair or deceptive acts and practices, and also enforces more than twenty-five other consumer protection statutes[3] and thirty regulations[4] that address such matters as consumer credit, telemarketing, and the sale of funeral goods and services. Combating fraud has been a top priority in fulfilling that mandate for over a decade. In particular, the Commission has committed significant resources to the war against telemarketing fraud -- a type of fraud that frequently victimizes the elderly.

Fraudulent marketing schemes change over time, but they share one thing in common: they all involve the use of deceptive or unfair practices to separate consumers from their money. Many fraudulent operations use the telephone as the primary means of communicating with their victims. Estimates of losses specifically caused by fraudulent telemarketers range from at least $3 billion to as much as $40 billion annually.[5] The Commission's law enforcement experience shows that telemarketing fraud victimizes consumers of all ages, levels of income, and backgrounds. The elderly, however, constitute a disproportionate number of telemarketing victims, and in some scams, 80 percent or more of the victims are 65 or older. The elderly often are the deliberate targets of fraudulent telemarketers who take advantage of the fact that many older people have cash reserves or other assets to spend on seemingly attractive offers.

Some older Americans seem especially susceptible to fraudulent offers for prize promotions and lottery clubs, charitable solicitations, and investment offers.[6]

Sections 5 and 13(b) of the Federal Trade Commission Act[7] provide the Commission with several important tools to combat various types of marketing fraud. These provisions authorize the Commission to file civil actions by its own attorneys in federal

district court and to seek an immediate halt to illegal activity. The Commission also seeks to obtain restitution for injured consumers, if possible; if not, the Commission seeks disgorgement of defendants' ill-gotten monies to the U.S. Treasury. Where appropriate, the Commission seeks an *ex parte* temporary restraining order, asset freeze and the appointment of a receiver to halt ongoing fraudulent activities and preserve assets for consumer redress. This extraordinary relief results in the immediate cessation of fraudulent telemarketing or other fraudulent schemes. Every year the Commission pursues such law enforcement activities to prevent hundreds of millions of dollars in fraud losses, and in the past three years, has collected over $61 million on judgments for consumer redress or disgorgement to the Treasury.

In 1994, Congress passed the Telemarketing and Consumer Fraud and Abuse Prevention Act (the "Telemarketing Act"), giving the Commission additional authority specifically to attack telemarketing fraud. At Congress' direction, the Commission promulgated the Telemarketing Sales Rule, which became effective on December 31, 1995. The Rule defines and prohibits deceptive telemarketing practices and prohibits other abusive telemarketing practices. One very important feature of the Telemarketing Act is that it permits a joint federal-state telemarketing enforcement strategy by enabling state Attorneys General to go into federal court to enforce the Telemarketing Sales Rule, to halt fraudulent schemes through nationwide injunctions against companies or individuals that violate the Rule, and to obtain restitution for injury caused to the residents of their states by the Rule violations. This grant of authority to the states has provided the Commission with an enormous opportunity to coordinate and leverage federal law enforcement resources with the states for maximum effect.

The Commission, working with its counterparts on the state level and its sister federal agencies, has developed a strategy of law enforcement "sweeps," in which multiple, simultaneous actions are filed all across the country against companies and individuals engaged in a particular type of fraud. Concentrating federal and state resources on a particular type of fraud to bring dozens of law enforcement actions at one time not only sends an emphatic warning to others engaged in the same fraud, it also provides a springboard to raise dramatically consumer awareness of that particular type of fraud. Since 1995, the Commission has led 56 cooperative law enforcement efforts focused upon the most prevalent types of fraud, including fraud that targets older consumers. These sweeps comprised a total of over 1,549 federal and state actions, including 365 cases brought by the Commission. I will describe some of these sweeps more specifically, as I discuss common varieties of marketing fraud.

Deceptive Prize Promotions and Lottery Clubs

One type of telemarketing fraud in which the victims are disproportionately elderly is the deceptive prize promotion. Typically, the consumer receives a call enthusiastically congratulating him or her on having been selected to receive a valuable award -- often described as thousands in cash, a car, a vacation, or jewelry. However, there is a "catch" that requires the consumer to send payment, often by an overnight courier service, in order to receive the prize. Then, although the consumer sends the payment as instructed,

he or she does not receive the promised valuable prize. If the consumer receives any award at all, it is generally an item of little or no value, such as inexpensive costume jewelry or a travel certificate that requires huge outlays of cash to redeem. Losses per consumer for telemarketed prize promotions generally range from a few hundred dollars to thousands of dollars. In some instances, consumers have lost their entire life savings to such scams. Although prize promotion telemarketers often ask for only a small amount initially, in a process referred to as "reloading," phone crooks request ever increasing amounts from consumers, promising ever more valuable awards. Once marked as receptive to this type of scam, a consumer often is bombarded with similar fraudulent offers from a host of scam artists. Prize and sweepstakes promotions remains one of the top five categories of complaints reported in the FTC's Consumer Sentinel - a multi-agency law enforcement investigative cyber tool.[8] Accordingly, fraudulent prize promotions have been a frequent target of Commission enforcement efforts. Since 1996, the Commission has led sweeps against prize promotions operators that have resulted in 80 enforcement actions against 119 defendants in 26 states.[9]

Prize promotions are not conducted exclusively through the telephone. In many cases, direct mail is used to capture the attention of the consumer. The Commission has taken action against several direct mail prize promoters, and joined other agencies in "Project Mailbox," begun in October 1997. Project Mailbox includes all types of fraudulent direct mail solicitations, but many of the actions targeted prize promotions. Project Mailbox involves the combined efforts of the FTC, the U.S. Postal Service, the Securities and Exchange Commission, and 25 state Attorneys General and local law enforcers, and, thus far, has resulted in a total of approximately 500 law enforcement actions.

Telefunders or Bogus Charities

Another type of telemarketing fraud, sometimes referred to as fraudulent "telefunding," targets consumers, often older citizens, willing to donate money to charitable causes.[10] Fraudulent telefunders, often employing prize promotions, either raise money for bogus charities, misrepresent the amount of donations that go to a bona-fide charity, or make other material misrepresentations about how the donor's money will be used. The Commission has brought several actions attacking alleged telefunding fraud and, again, has coordinated with other agencies to lead sweeps in this area.[11] To date, the effort has resulted in ten FTC cases and 86 state enforcement actions. At the Commission's press conference announcing the Operation Missed Giving sweep in November 1998, AARP released the results of a national survey on charitable giving habits of Americans, distributed a new educational video about telephone fundraising fraud, and operated a "reverse boiler-room," - a spin-off of the phone centers used by fraudulent telemarketers - manned by volunteer callers warning consumers that they may be targeted by deceptive charitable fundraisers and providing them with information on how to protect themselves from scams.

Business Opportunity Fraud

Many consumers -- particularly recent retirees or workers who have lost their jobs

through corporate downsizing -- are attracted to advertisements touting opportunities for individuals to operate their own small businesses or to work from home. In many cases, these business opportunities involve distributing products or services through vending machines or retail display racks. Calls from would-be entrepreneurs responding to these advertisements are connected to a telemarketer, who glowingly describes the opportunity and the amount of money that can be made by following the company's business plan. To clinch the sale, the telemarketer often provides the consumer with the names and telephone numbers of other people who have purportedly purchased the business opportunity and from whom the consumer can receive a supposedly objective opinion. In fact, these purported purchasers are "singers" -- individuals who are paid by the telemarketer to lie about the success of the business venture. After the consumer pays anywhere from hundreds to tens of thousand of dollars to become a distributor or to receive the business plan, he or she learns that the revenue projections of the telemarketer were highly inflated and that the only people who make money through the business opportunity are the telemarketers themselves.

Every year, the Commission brings numerous cases against purveyors of fraudulent business opportunities. In fact, the Commission's first major coordinated law enforcement initiative against fraud, "Project Telesweep," targeted such operations. Project Telesweep, launched in July 1995, used the combined efforts of the FTC, the U.S. Department of Justice, and several states to bring nearly 100 actions against alleged fraudulent business opportunities. The project was so successful that it served as a template for future telemarketing sweeps. Most recently, the Commission led "Project Bizillions", which was announced in January 2000. That sweep included 36 Commission cases and 33 state and local law enforcement cases.[12]

Recovery Scams

"Recovery" scams once plagued older consumers,[13] but this type of scam now appears almost to have vanished, due to aggressive enforcement efforts and tighter regulations.[14] Recovery scams were particularly egregious because they re-victimized consumers who had already fallen prey to one or more earlier scams. In a recovery scam pitch, the fraud operator offered to help the consumer obtain prizes promised in an earlier scam or to recover money lost in an earlier scam. After paying the fee for the recovery, the consumer never again heard from the recovery scammer - no refund, no prize, just the loss of more money. In some cases, the recovery scam operation was run by the very same individuals who previously defrauded the consumer. Losses per consumer victimized by recovery rooms ranged from a few hundred dollars to thousands of dollars.

Since the fall of 1994, the Commission has brought eight cases against recovery scam artists.[15] These enforcement actions, combined with provisions in the Telemarketing Sales Rule tailored specifically to prevent this type of fraud, have led to a dramatic drop in the number of consumer complaints. The Commission's consumer complaint database shows that complaints about recovery scams plunged by 95 percent from their high point in 1995 to their current low level.

Credit Card Loss Protection

In yet another telemarketing scam, fraud artists try to get people to buy worthless credit card loss protection and insurance programs. The telemarketers, who prey on elderly and young adults, scare consumers with false stories, telling them that they are liable for more than $50 in unauthorized charges on their credit card accounts; that they need credit card loss protection because computer hackers can access their credit card numbers through the Internet and charge thousands of dollars to your account, and that the telemarketer are from "the security department" and want to activate the protection feature on their credit card. This type of fraud affects senior citizens in particular. The National Consumer's League reported that a recent study of telemarketing fraud showed that 71 percent of the credit card loss protection plan complaints received by the National Fraud Information Center were made by consumers age 50 and older.[16] To address this problem, the Commission, since September 1999, has led sweeps resulting in four Commission cases and seven state cases against this type of fraudulent operation, including a criminal action by Florida law enforcement authorities.

The Internet

To date, most of the fraud affecting the elderly has been perpetrated through the telephone. As the elderly begin to use the Internet, fraud operators can be expected to find them through this new channel of communication and commerce. The Internet offers a novel and exciting means for all consumers to purchase both innovative and traditional goods and services faster and at lower prices, to communicate more effectively, and to tap into rich sources of information that were previously difficult to access and that now can be used to make better- informed purchasing decisions. The Internet's promise of substantial consumer benefits is, however, coupled with the potential for fraud and deception. Fraud operators are opportunistic, and therefore they are always among the first to appreciate the potential of a new technology. After buying a computer and modem, scam artists can erect and maintain a Web site for $30 a month or less, and solicit consumers anywhere on the globe. Most Internet fraud has clear antecedents in telemarketing fraud. What is different is the size of the potential market, and the relative ease, low cost, and speed with which a scam can be perpetrated.

The Commission believes it is important to address Internet fraud now, and in a manner that does not discourage legitimate commercial growth by undermining consumer confidence in the Internet as a safe mode of commerce. Toward that end, the Commission has filed more than 140 cases against 406 defendants whose alleged illegal practices involved the Internet. Most of the cases have involved old-fashioned scams dressed up in high-tech garb.[17] For seniors and their families surfing the Web for health information, one area of particular concern are health-related scams; old-fashioned snake oil salesmen also have gone online. To combat this problem, the Commission launched Operation Cure.All in June 1999, an ongoing federal and state law enforcement and consumer education campaign targeting false and unsubstantiated health claims on the Internet - - focusing in particular on claims for serious diseases such as arthritis, cancer, diabetes, heart disease, AIDS and multiple sclerosis.[18] To date, the FTC has filed seven

actions, sent more than 800 advisory letters to Internet companies making questionable health claims, and distributed tips to consumers on how to spot cyber health fraud and on how to find reliable health information online.

In addition to overall Internet-related law enforcement efforts, the Commission has developed comprehensive consumer and business education initiatives, including Surf Days to inform entrepreneurs about online problems and "teaser" pages to warn consumers about specific scams.[19]

Additional Approaches to Combating Fraud

Assisting Criminal Authorities

The Commission also combats telemarketing fraud by providing substantial resources to enforcement efforts coordinated by criminal authorities. The FTC assigned eight attorneys to the Chattanooga, Tennessee Telemarketing Fraud Task Force in 1995. Chattanooga had become a leading center of fraudulent telemarketing activity, particularly prize promotion scams. The overwhelming majority of the victims of the Chattanooga operations were elderly. The FTC attorneys were cross-designated as Special Assistant U.S. Attorneys and brought criminal actions against telemarketers operating in the area. By the end of 1996, the Chattanooga Task Force had obtained fifty convictions and combined prison sentences against fraudulent telemarketers totaling over 1,695 months and restitution orders in excess of $35 million.[20] Because the defendants targeted vulnerable victims, including the elderly, their prison sentences were enhanced.[21]

The FTC also participated in a cross-border project in Harrisburg, Pennsylvania where staff assisted in an ongoing crackdown on fraudulent telemarketing schemes based in Canada that targeted victims in the U.S. The defendants mainly telemarketed investments. Since 1995, 125 defendants, including 97 Canadian nationals, have been charged criminally, and more than $4 million has been recovered for restitution to U.S. consumers. And in December 1998, FTC staff assisted a criminal prosecution of a recovery room operation. Many of the approximately 850 victims, who paid defendants more than $1.6 million, were elderly. The owner was sentenced to 63 months in jail, the managers were sentenced to jail terms between 21 to 36 months, and the telemarketers were sentenced from 6 months home detention to 21 months in jail.[22]

The Commission assisted in the recent prosecution of perpetrators of investment schemes based in New Hampshire, including the prosecution of a former U.S. Attorney who, in June 2000, was sentenced to 24 months in prison.[23] In one of these cases, the telemarketers convinced victims to switch their existing Individual Retirement Accounts to a worthless wireless cable investment.

In addition, the Commission participated in Operation Senior Sentinel, announced in December 1995, which, with over 400 arrests in 14 states, was the largest criminal crackdown ever on telemarketing fraud and focused specifically on scams targeting older

Americans. Estimates indicate that nearly 80 percent of the victims in the underlying prize promotion and recovery room cases included in Senior Sentinel were older people. The FTC contributed valuable consumer complaint information to Senior Sentinel and also filed five civil cases in federal district court -- four against alleged fraudulent prize promotions and the fifth against an alleged recovery room.

Consumer Sentinel and the Consumer Response Center

The Commission realizes that coordination and information sharing are key to effective consumer protection law enforcement. *Consumer Sentinel*, a secure database developed by the FTC and now shared with over 250 law enforcement agencies in the U.S. and Canada, puts this concept to work. Currently containing more than 250,000 entries, the database allows law enforcement from local sheriffs to the FBI to identify companies and individuals engaging in fraud and to stop scams as they emerge. As the Internet makes cross-border transactions more commonplace, we have recognized the importance of global information sharing. Recently, the Commission entered into an agreement with our Australian counterpart, the Australian Competition and Consumer Commission, to share information through Sentinel, and cooperate in law enforcement efforts. The Commission intends to continue to recruit domestic and foreign consumer protection agencies as Sentinel partners, allowing all to use these resources efficiently and in concert.

Much of the complaint data in the Sentinel system comes directly from consumers who contact the agency. Consumers have toll-free access to the FTC's Consumer Response Center through a consumer helpline. Launched in July 1999 with additional funds appropriated by Congress, 1-877-FTC-HELP allows people from anywhere in the United States to call with questions or complaints and speak to trained counselors. Our Web site, www.ftc.gov, provides an online complaint form, and some complaints reach us through postal mail. The FTC now receives more than 10,000 consumer inquiries or complaints each week.

The agency's data collection and analysis function expanded in 1998 when Congress enacted the Identity Theft and Assumption Act. This law empowered the FTC to collect identity theft complaints, and refer them to law enforcement entities for prosecution. In response, we established the Identity Theft Data Clearinghouse, a component of Consumer Sentinel which contains consumer complaints about this rising crime. Calls to the dedicated identity theft hotline (1-877-ID THEFT) now exceed 1,000 a week, marking a steady increase since the hotline was launched in November 1999. Consumers who call this line are connected to counselors who are specially trained in the intricacies of identity theft and the credit laws. These counselors give pertinent information to callers, assisting them to repair the damage inflicted by the identity thieves. The database now contains close to 15,000 entries, and is available to law enforcers through the secure Sentinel site.[24]

Cooperative Efforts with Older Consumers

The Commission and other law enforcement agencies have taken advantage of the fact that many older consumers are eager to help combat fraud. In an effort that began several years ago, many older consumers, whose names had found their way onto lists used by fraudulent telemarketers, have agreed to tape record telemarketing calls they receive or to turn over their old telephone numbers so that undercover investigators can tape the telemarketers' pitches. When a law enforcement agency receives a tape of a telemarketing sales pitch, the agency notes that a tape of the encounter is available and shares that information with other law enforcers through a program known as the National Tape Library. The Commission and other law enforcement agencies have used these tapes effectively in law enforcement actions because they are often incriminating and capture precisely the misrepresentations made by the telemarketer. Through the Commission's Consumer Sentinel database, the index of the National Tape Library is now accessible by means of the Internet to authorized law enforcement agencies, making it significantly easier for consumer protection agencies to learn of and share this incredibly valuable evidence.

In a similar effort to enlist older consumers in the fight against fraud, the Commission has joined with other law enforcers and AARP to form a public/private strike force to collect and review direct mail for future law enforcement purposes. Volunteers have agreed to send suspicious or fraudulent direct mail offers to AARP, where information about the offers will be entered into a database shared with law enforcement authorities.

Consumer Education

Consumer education is an effective protection against fraud. To leverage expertise and limited resources, the FTC has developed the Partnership for Consumer Education, a group of over 90 corporations, trade groups, consumer organizations, and federal agencies that works with us to distribute effective consumer education materials to fight fraud. With the assistance of our partners, the Commission has arranged for messages about fraud to appear in such diverse locations as sales catalogs, billing statements, classified advertising, and even on public transit buses.

It is especially important for older consumers to know their rights and learn how to assert those rights when dealing with telemarketers. To reach out to seniors in informal settings, the Commission's has coordinated local events with partners such as the Florida Attorney General's Office, AARP, local BBBs. The FTC's primary focus has been on southern states to reach retired seniors in particular. Since July 1999, the Commission has hosted or participated in seven such events, including an Elder Fraud Conference for consumer advocates, senior leaders and law enforcement in Florida, a consumer awareness forum for minority seniors, and a Consumer University discussing such topics as telemarketing fraud, identify fraud, charity fraud, door-to-door frauds, home repair, mail fraud and Internet fraud.

The Commission's creative and plain English consumer education publications - - most of which are available at the FTC's Web site ftc.gov - - provide advice and tips on a wide range of consumer topics. The publications advise that if a consumer does not wish to

receive subsequent calls from a particular company, the consumer should ask to be placed on the company's "do-not-call" list. The publications further advise that it is an unlawful practice for a telemarketer to call a consumer who has indicated that he or she does not wish to receive calls from the selling organization. The Commission's consumer education materials also inform that the law requires telemarketers to disclose the seller's identity and that the purpose of the call is to sell goods or services. The materials state that consumers should be extremely wary whenever they receive a call from a telemarketer who does not promptly disclose this information. One theme that is stressed in the FTC's consumer education materials is that consumers should hang up on any telemarketer who tells them that they need to send in payment to receive an award or to participate in a prize promotion. The Commission attempts to get the message to consumers that they do not have to pay money to enter a sweepstakes or prize contest. Another important theme is that consumers should never divulge their credit card numbers or checking account numbers over the phone unless they have agreed to make a purchase and they understand the terms of the purchase. The only reason a company ever needs a consumer's credit card or checking account number is to bill the consumer for the purchase. Also, the Commission's consumer education materials note that whenever possible, consumers may wish to make purchases by credit card so that they will have the protections afforded to such transactions by federal law. If the company fails to deliver goods or services paid for by credit card, the consumer is entitled to dispute the charge with the organization that issued his or her credit card, which is obligated to conduct an investigation of the consumer's complaint. Depending upon the result of that investigation, the consumer may be eligible for a credit or refund of the purchase price.

Another important point stressed in the Commission's consumer education materials is that consumers should be on the alert for high-pressure tactics or demands from a telemarketer for an immediate purchasing decision. The materials also advise consumers to consider carefully any offer, to review any written materials, and to seek out advice from family or friends before making an expensive purchase. If consumers are interested in reducing the number of solicitations they receive in the mail or by telephone, they may wish to contact the Direct Marketing Association ("DMA"), a private trade association that voluntarily maintains and supplies to its members lists of consumers who have indicated they do not wish to receive solicitations. Not all direct marketers use the DMA list to screen out consumers. Therefore, contacting DMA will not eliminate the receipt of mail and telephone solicitations, but it may help reduce the volume. The DMA's address is available via the Internet on the Commission's Web site or through the Commission's Consumer Response Center. Consumers can contact the Federal Trade Commission or the state Attorneys General if they lose money to a company engaged in fraud or even if they receive a solicitation which they believe is misleading or suspicious. Although the Commission does not intervene in individual disputes, consumer complaints provide vital information that the Commission uses in developing its enforcement agenda and in determining whether a particular company is engaged in a pattern of deceptive practices or fraud, making it a suitable target for legal action.

Conclusion

The Commission's fraud program is of special interest and importance to this country's senior citizens, because the elderly often find themselves victimized by such operations. The Commission will remain alert to new schemes that target senior citizens and will continue its aggressive campaign against telemarketing fraud to prevent injury to all consumers, including the elderly.

1. The views expressed in this statement represent the views of the Commission. However, my oral testimony and responses to questions are my own and do not necessarily reflect the Commission's views or the views of any Commissioner.

2. 15 U.S.C. §§ 41 et seq.

3. E.g., the Truth in Lending Act, 15 U.S.C. §§ 1601 et seq., which mandates disclosures of credit terms; the Fair Credit Billing Act, 15 U.S.C. §§ 1666 et seq., which provides for the correction of billing errors on credit accounts; the Fair Credit Reporting Act, 15 U.S.C. §§ 1681 et seq., which establishes rights with respect to consumer credit reports; the Magnuson-Moss Warranty Act, 15 U.S.C. §§ 2301 et seq., which provides disclosure standards for consumer product warranties; and the Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101-08, which authorizes the Commission to promulgate rules defining and prohibiting deceptive telemarketing practices and other abusive telemarketing practices.

4. E.g., the Telemarketing Sales Rule, 16 C.F.R. Part 310, which defines and prohibits deceptive telemarketing practices and other abusive telemarketing practices; the Care Labeling Rule, 16 C.F.R. Part 423, which requires the provision of care instructions for wearing apparel; the Franchise Rule, 16 C.F.R. Part 436, which requires the provision of information to prospective franchisees; the Mail and Telephone Order Merchandise Rule, 16 C.F.R. Part 435, which gives consumers certain rights when ordering products through the mail; and the Funeral Rule, 16 C.F.R. Part 453, which regulates certain pricing and sales practices by funeral providers.

5. See, Committee on Government Operations, *The Scourge of Telemarketing Fraud: What Can Be Don Against It?*, Fifteenth Report by the Committee on Government Operations (U.S. G.P.O.: 1991), at p. 7 ("Various estimates place losses to consumers each year from telemarketing fraud at $3 billion to $15 billion to $40 billion and probably hundreds of millions of dollars to financial institutions.").

6. Recent survey research conducted on behalf of AARP shows that there is no ready answer explaining why a disproportionate number of telemarketing fraud victims are elderly. The research rebuts the notion that the elderly are vulnerable because they are socially isolated, ill-informed, or confused. The survey shows, however, that older people who fall for telemarketing scams tend to believe the pitches they hear -- that they have a good chance of actually winning the grand prize, and that the products touted are worth the price charged for them. Ninety percent of respondents report awareness of consumer fraud; yet two-thirds said it is hard to spot fraud when it is happening. The survey also shows that elderly victims find it difficult to terminate telephone conversations, even when they say they are not interested in continuing a conversation. They are also reluctant to seek advice or assistance from others about financial matters in general.

7. 15 U.S.C. §§ 53(b) and 57b.

8. Consumer Sentinel is discussed *infra* at p. 14.

9. Project Prize Fighter, announced in July 2000, included 3 FTC actions and 11 criminal actions among the 21 actions brought by the U.S. Postal Inspection Service, Attorneys General from five states, and two local law enforcement authorities. In addition, the eight cases the Commission brought in connection with Operation Jackpot in 1996 resulted in the defendants paying more than $550,000 in consumer redress or

disgorgement to the U.S. Treasury.

10. The Commission examined demographic data on the victims of five telefunding operations the Commission sued in 1994 and found that out of 143 consumers interviewed, 85 percent were at least 65 years of age.

11. See FTC v. North American Charitable Services, Inc., Civil No. SACV 98- 968 LHM (EEx)(C.D. Cal. filed Nov. 9, 1988); FTC v. Eight Point Communications, Inc., Civil No. 98-74855 (E.D. Mich. filed Nov. 10, 1998); FTC v. Leon Saja, d/b/a Southwest Publishing, Civil No. CIV 97-0666 PHX sm (D. Ariz. filed March 31, 1997); FTC v. The Baylis Co., Civil. No. 94-0017-S-LMB (D. Idaho filed Jan. 10, 1994); FTC v. NCH, Inc., Civil No. CV-S-94-00138-LDG (LRL) (D. Nev. filed Feb. 14, 1994); FTC v. International Charity Consultants, Civil No. CV-S-94-00195-DWH (LRL) (D. Nev. filed Mar. 1, 1994); FTC v. United Holdings Group, Inc. (D. Nev. 1994); FTC v. Voices for Freedom, Civil No. 91-1542-A (E.D. Va. filed Oct. 21, 1991).

12. A number of the Commission's cases sought injunctions against the defendants' failure to comply with the Commission's Franchise Rule, 16 C.F.R. Part 436, which requires sellers of franchises and business opportunities to provide prospective purchasers with disclosures covering 20 specified material topics, including the names and addresses of current and former owners of the franchise or business opportunity.

13. In its investigation of one recovery room case, SCAT, Commission staff interviewed 43 consumers who were allegedly victimized or approached by SCAT telemarketers. Of these individuals, 81 percent were at least 65 years of age; 47 percent were at least 75; and 23 percent were at least 80. Similar percentages have been found in other recovery room cases.

14. The Telemarketing Sales Rule expressly prohibits telemarketers from requesting or accepting payment for "recovery" services until 7 business days after the promised goods, services, or cash have been recovered and delivered to the consumer. 16 C.F.R. § 310.4(a)(3).

15. FTC v. Telecommunications Protection Agency, Inc., Civil No. CIV-96-344-5 (E.D. Okla. filed July 24, 1996); FTC v. Desert Financial Group, Inc., Civil No. CV-S-95-0151-LDG (D. Nev. filed Dec. 5, 1995); FTC v. Meridian Capital Corp., Civil No. CV-S-96-00063-PMP (D. Nev., transferred to D. Nev. Jan. 23, 1996, originally filed in D.D.C Aug 17, 1995); FTC v. USM Corp., Civil No. CV-S-95-0668-LDG (D. Nev. filed July 12, 1995); FTC v. PFR, Civil No. CV-S-95- 000745-HDM (D. Nev. filed Jan. 25, 1995); FTC v. Thadow, Inc., Civil No. CV-S-95-00074-PMP (D. Nev. filed Jan. 25, 1995); FTC v. United Consumer Services, Civil No. 1:94-CV-3164-CAM (N.D. Ga. filed Nov. 30, 1994); FTC v. Richard Canicatti, d/b/a Refund Information Services, Civil No. CV-S-No. 94-859-HDM (D. Nev. filed Oct. 11, 1994).

16. The study, summarized in a comment submitted to the Commission that is available at www.ftc.gov/bcp/rulemaking/tsr/comments/index.html, also stated that consumers age 50 and older accounted for 38 percent of their telemarketing fraud complaints across all categories.

17. For a comprehensive overview of the Commission's Internet law enforcement activities, including a list of cases, see *Five Years: Protecting Consumers Online*, available at www.ftc.gov/opa/1999/9912/fiveyearreport.htm.

18. As part of Operation Cure.All, in June 2000, the Commission announced a $1 million settlement with Lane Labs USA, Inc., resolving allegations of false and unsubstantiated claims about the company's shark cartilege and skin cream marketed to consumers as cancer treatments (FTC v. Lane Labs USA, Inc., Civil No. CV-00-3174 (WGB) D. N.J. filed June 28, 2000). Other Cure.All cases include Michael D. Miller, d/b/a Natural Heritage Enterprises, Docket No. C-3941 (May 16, 2000); CMO Distribution Centers of America, Docket No. C-3942 (May 16, 2000); EHP Products, Docket No. C-3940 (May 16, 2000); Arthritis Pain Care Center, Docket No. C-3896 (Sept. 7, 1999); Body Systems Technology, Inc., Docket

No. C-3895 (Sept. 7, 1999).

19. Knowing that many consumers use the Internet to shop for information, agency staff have developed "teaser" sites that mimic the characteristics that make a site fraudulent. Metatags embedded in the FTC sites make them instantly accessible to consumers who are using major search engines and indexing services as they look for products, services, and business opportunities. Within three clicks, the "teaser" sites link back to the FTC's site. There, consumers can find the practical information they need to learn to recognize fraudulent claims. The agency has developed 13 such "teaser" sites on topics ranging from health care products to scholarship services to vacation deals and investments, and feedback from the public has been overwhelmingly positive.

20. In recognition of the FTC's contributions, the U.S. Department of Justice honored the FTC attorneys with its John Marshall Award for inter-agency cooperation in support of litigation in 1996.

21. See 18 U.S.C. § 2236 for enhanced penalties for any telemarketer convicted of victimizing ten or more persons over the age of 55 or targeting persons over the age of 65. The United States Sentencing Guidelines also increase sentences for any convicted criminal that targets victims according to age. See, USSG § 3A1.1.

22. *United States v. Jeffrey Jordan et al.*, CR-S-96-113-LRL (D. Nev. filed 1997; subsequently transferred to D.D.C.).

23. For a description of the case, see "Ex-Regulator Sentenced in Telemarket Fraud," *The New York Times*, July 18, 2000 at C2.

24. The Consumer Sentinel complaint form does not ask for the caller's age. Identity theft callers have the option of providing age information. About 55% of victims calling the identity theft hotline report their age. Of these, 40% fall between the 30 and 44 years of age. Approximately 26% are between age 45 and 64, and another 25% are between age 19 and 29. About 7% of those reporting their ages are 65 and over; and slightly over 2% are age 18 and under.

Exhibit M

RESEARCH REPORT

TRUSTe 2014 US Consumer Confidence Privacy Report

Consumer Opinion and Business Impact

CONSUMER
CONCERN

CONSUMER
TRUST

BUSINESS
IMPACT

TRUSTe Inc.

US: 1-888-878-7830

www.truste.com

EU: +44 (0) 203 078 6495

www.truste.eu

INTRODUCTION

2013 saw privacy become a mainstream concern.

The year saw revelations about government surveillance programs such as PRISM, continued debate over "Do Not Track," the introduction of new FTC Mobile guidelines, changes to the Children's Online Privacy Protection Act (COPPA) and European concern over international data transfers under EU Safe Harbor to name but a few.

It concluded with the United Nations passing a privacy resolution on "The Right to Privacy in the Digital Age," and President Obama announcing changes to the National Security Agency (NSA) practice of bulk data collection and storage and, in Europe, the debate over the proposed new Data Protection Regulation intensifying ahead of the end of the current parliament in May 2014.

Technological advances also brought new privacy implications including the introduction of wearable tech such as Google Glass, commercial use of facial recognition technology to track shoppers' in-store activities, increased use of location-based targeting and the rise of smart devices in what's being called "The Internet of Things."

But what is the impact of these new technologies, political debates and media headlines on consumer opinion?

As part of our commitment to helping companies to safely collect and use consumer data to power their businesses, we wanted to get behind the headlines and find out what effect the events of 2013 have had on consumer privacy concerns and provide an accurate picture of the potential impact this could have on businesses in the year ahead.

TRUSTe commissioned independent research to look into the degree and causes of online privacy concern amongst US internet users. The TRUSTe 2014 US Consumer Confidence Research is part of a long-term commitment to privacy education from TRUSTe. Now in its third year, this research series offers a valuable barometer of consumer confidence, business impact and recommended business practices.

Reports from previous years can be found online at truste.com. The 2014 findings will be presented at a series of events in the US and the UK to coincide with Data Privacy Day on January 28.

If you have questions on the research, or would like additional information on how TRUSTe can help you with your data privacy management strategy, please let us know.

Best Regards,

Chris Babel
CEO, TRUSTe

EXECUTIVE SUMMARY

The TRUSTe 2014 US Consumer Confidence Privacy Report provides a comprehensive analysis of current consumer opinions about online privacy across the US. The study was conducted by Harris Interactive, on behalf of TRUSTe, with more than 2,000 US internet users from December 11 – 13, 2013. A similar report is also available for the UK.

The research found that consumer online privacy concerns remain extremely high with 92% of US internet users worrying about their privacy online compared with 89% in January 2013. The high level of concern is further evidenced by 47% saying they were always or frequently concerned and 74% were more concerned than last year.

All those who said they were more concerned about their online privacy than last year were asked why they were more concerned. The top two responses were - 58% were concerned about businesses sharing their personal information with other companies and 47% were concerned about companies tracking their online behavior to target them with ads and content.

Despite the constant media coverage of US government surveillance programs only 38% listed this as a reason for their increased concern. These figures are in stark contrast to the number of media articles about online privacy, which focus on government surveillance over commercial data collection.

The potential impact of this concern over business privacy practices is significant as consumer trust is falling. Just over half of US internet users (55%, down from 57% in 2013) say they trust businesses with their personal information online. Furthermore, 89% say they avoid companies they do not trust to protect their privacy, the same as in January 2013.

70% said they felt more confident that they knew how to manage their privacy than one year ago, but this can cause consumers to take actions, which negatively impact businesses. Increased privacy concerns, mean consumers are:

Less likely to click on online advertisements	83%
Avoid using apps they don't believe protect their privacy	80%
Less likely to enable location tracking on smartphone	74%

On a positive note, in addition to these actions, 3 out of 4 consumers are more likely to look for privacy certifications and seals to address their privacy concerns.

TRUSTe 2014 US CONSUMER CONFIDENCE PRIVACY RESEARCH

Survey Methodology

The research was conducted by Harris Interactive on behalf of TRUSTe, from December 11-13, 2013.

Questions were asked online of 2,019 adults aged over 18.

The survey data were weighted to be nationally representative of the US Online Adult Population.

Numbers may not always add up to 100% due to computer rounding or multiple answers. Full data tables are available on request.

DETAILED FINDINGS

Section 1 — Consumer Concern

1.1   Are consumers concerned about online privacy?

Consumer online privacy concerns remain high. 92% of US internet users worry about their privacy online compared with 89% in January 2013 and 90% in January 2012.

Of the 92% who are concerned about their online privacy, 18-34 aged men are less likely to worry (83%) than women of the same age (93%). Men aged 65+ are more likely to be concerned (97%) than women of the same age (91%).

"How often do you worry about your privacy online?"
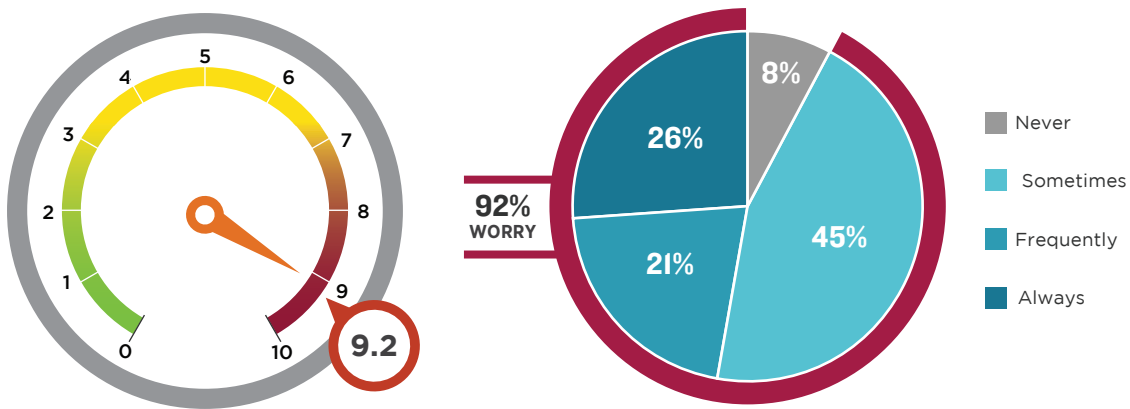
1.2   How often are they concerned about online privacy?

What is the extent of privacy concern? Respondents were asked how often, if at all, they worried about their online privacy. 47% said they were always or frequently concerned, 45% were sometimes concerned. Just 8% have never worried about the issue compared with 11% in January 2013.

1.3   What online activities cause them to be concerned?

This research was conducted in mid-December during the peak of the holiday shopping season. Online shopping continues to be the activity that causes the greatest levels of concern with 93% of US consumers now worried about their privacy when shopping online, compared with 89% in January 2013.

5

Privacy concerns have also increased across other online activities. 90% were concerned about privacy when banking online compared with 86% in January 2013. 90% of those who used social networks worried about their privacy when using these sites compared with 87% in January 2013.

There has also been a significant rise in privacy concern when using mobile apps, with 85% of smartphone users now worried when using apps compared with 77% in January 2013.

Activities Where Consumers have Privacy Concerns

Activity	2013	2014
Online Shopping	89%	93%
Banking Online	86%	90%
Using Social Media	87%	90%
Using Mobile Apps	77%	85%
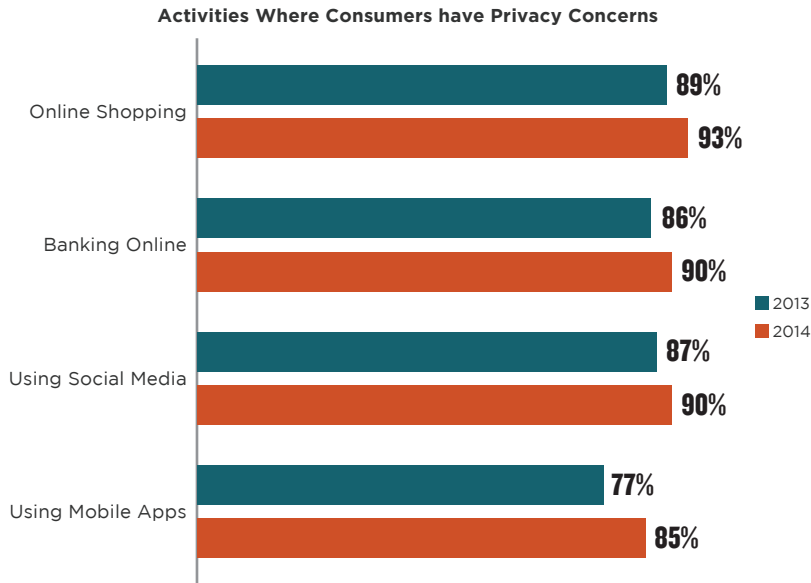
1.4   Has concern about online privacy increased since last year?

Respondents were asked about whether their privacy concerns had changed from one year ago. 74% of US internet users are more worried about their online privacy than one year ago.

74% of internet users are more worried about online privacy than one year ago

74%

A higher percentage of those over age 55 (78%) are more worried about their online privacy than one year ago. The groups that are least concerned compared with last year are men aged 18-34 (67%) and women aged 35-44 (69%).

Perhaps surprisingly, the increase in privacy concerns is lower (66%) in families with children compared to those without (77%). Other factors such as income, education, employment, marital status and home ownership appear to make little difference to growing online privacy concerns.

Section 2 — Reasons for Concern

2.1   Why have online privacy concerns increased?

All of the respondents who indicated that they were more concerned about their online privacy this year than last year (74%) were asked what had caused them to be more concerned.

Businesses sharing personal information with other companies (58%) and tracking online behavior to show targeted ads and content (47%) were the two largest causes of increased online privacy concerns.

Despite the constant media coverage of US government surveillance programs such as the NSA's PRISM, only 38% listed this as a reason for their increase in privacy concerns.

29% were concerned about the privacy policies of Facebook and other social media networks, 24% were concerned about companies tracking their location on their smartphone and 21% were concerned about the privacy policies of Google and other search engines.

Top 6 Reasons for Increase in Online Privacy Concerns in 2013

Reason	Percentage
Businesses sharing my personal information with other companies	58%
Companies tracking my online behavior to target me with ads and content	47%
Reports of government surveillance programs (e.g. NSA, PRISM) in the media	38%
Privacy policies of Facebook and other social media sites	29%
Companies tracking my location via my smartphone	24%
Privacy policies of Google and other search engines	21%

2.2   Does everyone share the same reasons for concern?

There were some differences in the causes of concern in different age groups. Businesses sharing personal information online with other companies, was the top cause of concern amongst all age groups apart from 18-34 year old men who were more concerned about government surveillance programs.

The second highest cause of concern for everyone over 35 was companies tracking their online behavior to provide targeted ads and content. For 18-34 year olds the second highest cause of concern was government surveillance followed by online tracking.

2.3   Detailed analysis of top causes of privacy concerns

2.3.1   Businesses sharing personal information with other companies

Overall 58% of those whose concerns about online privacy had increased in the last year listed businesses sharing personal information with other companies as a cause.

This was the greatest concern for retired people (74%) followed by those who left education after high school (63%) and the unemployed (63%).

Concerns increase sharply with age with 42% of 18-34 year olds listing companies sharing personal information as a reason for concern, rising to 74% of 65+ year olds.
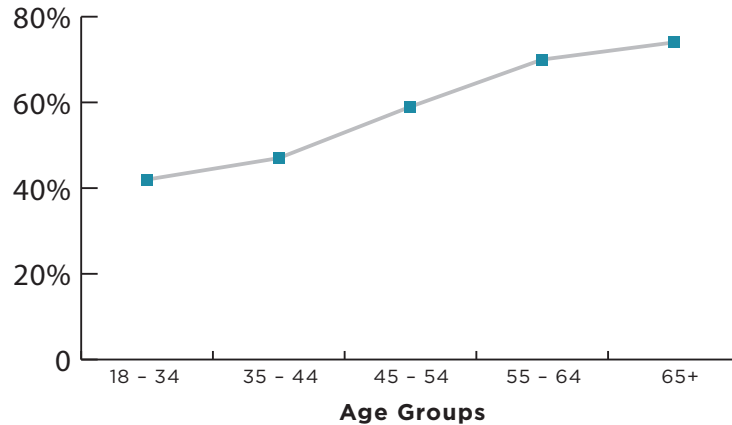
The greatest level of concern (76%) was amongst women aged over 65. 62% of married people were concerned about businesses sharing their personal information compared with 52% of those who were not married.

2.3.2   Companies tracking online behavior to provide targeted ads and content

Concerns about companies tracking online behavior to provide targeted ads and content increased sharply with age and peaked amongst those aged 55-64.
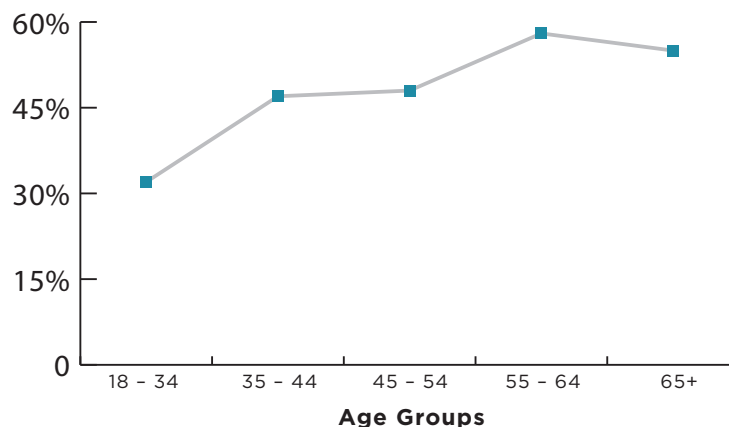
Online tracking to provide targeted ads and content was less of a concern amongst students (37%) than for retired people (55%).

53% of married people were concerned about companies tracking online behavior to provide targeted ads and content compared with 40% of those who were not married.

TRUSTe   **POWERING TRUST in the Data Economy**

CONTACT US   US: 888.878.7830   www.truste.com | EU: +44 (O) 203 078 6495   www.truste.eu

2.3.3   Media reports of government surveillance programs such as NSA's PRISM

Overall 38% of those whose online privacy concerns had increased over the last year attributed this to media reports of government surveillance programs such as the NSA's PRISM program.

This was the third highest concern for 35-65 year olds. For 18-34 year olds and those over 65 government surveillance was their second highest concern and more of a concern than online tracking.

In general, men were more concerned about government tracking them (44%) than companies (38%) whereas women were more concerned about companies tracking their activities (41%) than the government (32%).

Students (43%) were also more concerned about reports of surveillance programs (43%) than companies tracking their web surfing behavior (29%).

2.3.4   Privacy policies of Facebook and other social media sites

Overall 29% of internet users attributed their increase in online privacy concern to the privacy policies of Facebook and other social media sites. However these concerns were greater amongst certain groups rising to 36% of college graduates and 34% for parents of children under 18.

2.3.5   Companies tracking my location data via my smartphone

Overall 24% of internet users attributed their increase in online privacy concern to companies tracking their location via their smartphone. These concerns were significantly higher amongst younger people whether male or female.
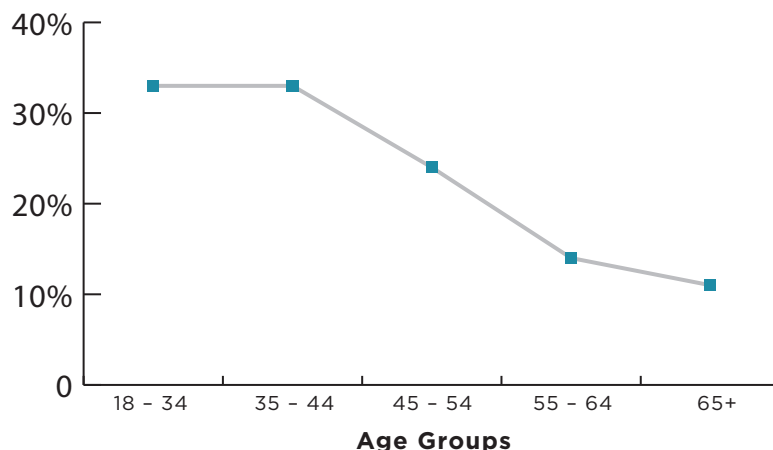
These figures are based on all internet users so are likely to be significantly higher as a proportion of smartphone users.

2.3.6   Privacy policies of Google and other search engines

21% of internet users listed the privacy policies of Google and other search engines as a reason for the increase in their online privacy concerns. For younger people this is the lowest concern, however for over 55 year olds this is more of a concern than location-based tracking. This is particularly the case amongst older men. 29% of men aged 55-64 are concerned about Google's privacy policies, whereas location based tracking is only a concern for 16% of this age group.

Section 3 — Consumer Trust

3.1   Do consumers trust companies to protect their online privacy?

Consumer trust decreased from last year. 55% of US internet users trust businesses with their personal information online, compared with 57% in January 2013 and 59% in January 2012.

In general, men over 45 are less likely to trust companies with their personal information online than women of the same age. For example, 53% of men aged 55-64 do not trust companies with their personal information compared with 39% of women of the same age.

"I trust most companies with my personal information online."
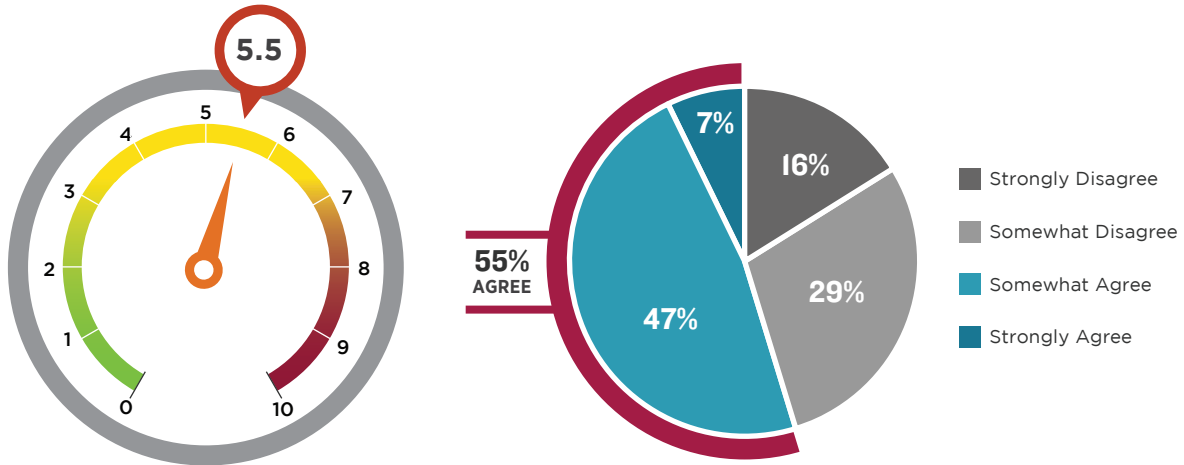
3.2   What is the level of consumer mistrust?

Respondents were asked to what extent they agreed with the statement "I trust most companies with my personal information online." 45% strongly or somewhat disagreed with this statement, 47% somewhat agreed. 7% strongly agreed that they trusted most companies with their personal information online compared with 9% in January 2013.

Section 4 — Business Impact

4.1 Business impact of online privacy concerns

The business impact of online privacy concerns remains high. 89% of US internet users say they avoid companies that do not protect their privacy compared with 89% in January 2013 and 88% in January 2012.

When it comes to avoiding companies where consumers have online privacy concerns, there is little difference between men and women but age is a major factor. 83% of 18-34 year olds avoid businesses they do not trust rising to 96% of over 65 year olds.

"I avoid doing business with companies who I do not believe protect my privacy online."
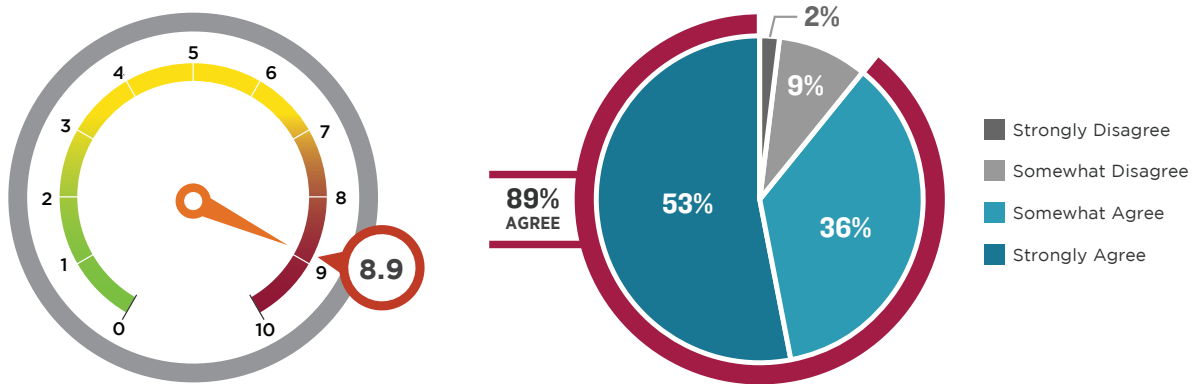
4.2 To what extent do consumers avoid businesses they don't trust?

Respondents were asked to what extent they agreed with the statement "I avoid doing business with companies who I do not believe protect my privacy online." 53% strongly agreed with this statement, 36% somewhat agreed, 9% somewhat disagreed. 2% strongly disagreed that they avoided doing business with companies that they didn't believe protected their privacy online.

4.3 Effects of privacy concern on consumer behavior

70% of US internet users feel more confident that they know how to manage their privacy online than one year ago but what does this mean for businesses? As consumers become smarter about managing their privacy and decide to opt out of services such as location tracking, could this hinder business' ability innovate? A series of additional questions were asked this year that looked in more detail at the potential business impacts of consumer online privacy concerns.

Enabling consumers to take control of their online privacy can help with 76% consumers more likely to look for privacy certifications and seals to address their privacy concerns.

Top 4 Consumer Actions due to Online Privacy Concerns
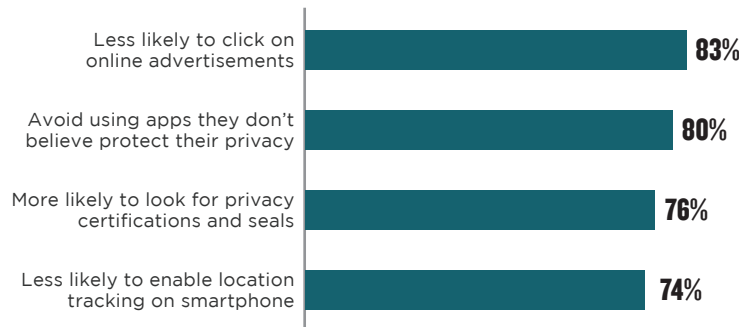
CONCLUSION

Businesses Need To Do More To Build Online Trust

Privacy concerns are growing with 74% more concerned about their online privacy than a year ago. Despite the constant media coverage of US government surveillance programs such as NSA's PRISM, this is not the main driver of online privacy concerns. People are far more concerned about businesses sharing personal information with other companies and tracking their online behavior to show targeted ads and content than anything the government is doing.

Many companies have already responded to growing consumer concern and are improving their privacy practices, but the bar continues to rise. For those who have not yet realized the importance of this issue, they are going to be left behind by their competitors.

But consumer concern is just one of the challenges businesses face in 2014 as the privacy landscape continues to get more complex in terms of regulation and technology. 2013 saw changes to the COPPA, continued debate over "Do Not Track," the introduction of new FTC Mobile guidelines and European concern over international data transfers under EU Safe Harbor.

The good news is that there are a number of different ways in which businesses can help consumers to manage their online privacy and build trust. These include privacy assessments and certifications to build and demonstrate best practices, alongside tools for managing consumer advertising preferences, monitoring site and app tracking activity, and cookie consent preferences under the EU Cookie Directive. This research showed that 76% are more likely to look for privacy certifications and seals due to concerns about their online privacy.

In the year ahead, companies need to innovate to succeed but these findings show they also need to proactively address online privacy concerns to stay ahead of the competition, minimize risk and build online trust.

ABOUT TRUSTe

TRUSTe is the leading global Data Privacy Management (DPM) company and powers trust in the data economy by enabling businesses to safely collect and use customer data across web, mobile, cloud and advertising channels. Our cloud-based Data Privacy Management Platform delivers innovative technology products, including website monitoring and advertising compliance controls – along with privacy assessments and certifications.
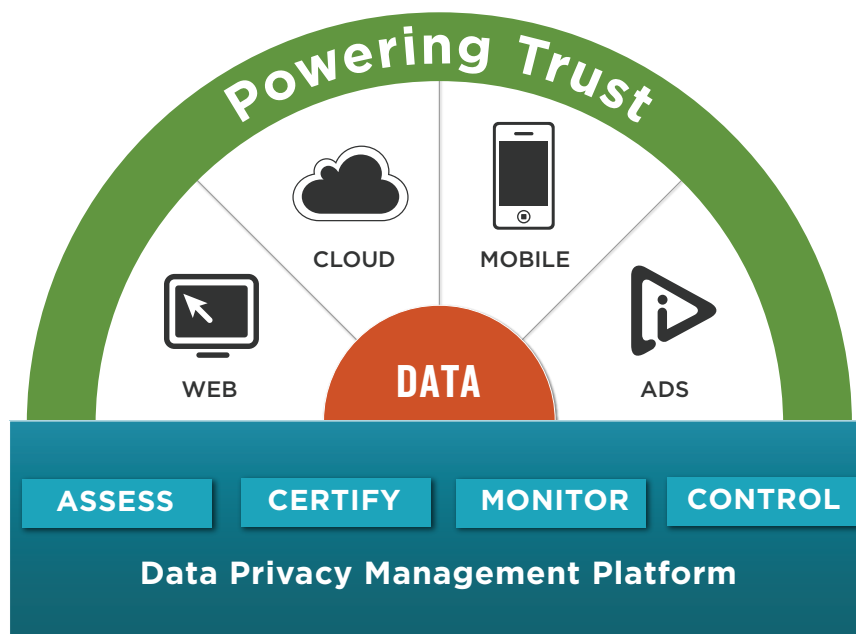
More than 5,000 companies worldwide, including Apple, Disney, eBay, Forbes, LinkedIn and Oracle rely on our DPM platform and globally recognized Certified Privacy Seal to protect/enhance their brand, drive user engagement and minimize compliance risk.

FURTHER INFORMATION

A full list of TRUSTe's Privacy Research reports, including the Consumer Confidence Privacy Indexes for 2013 and 2012, can be found at www.truste.com/resources/#/Privacy_Research.

For more information, please see www.truste.com or contact eleanor@truste.com

TRUSTe

POWERING TRUST in the Data Economy

CONTACT US   US: 888.878.7830   www.truste.com | EU: +44 (0) 203 078 6495   www.truste.eu

Exhibit N

The New York Times | https://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html

Start-Ups Seek to Help Users Put a Price on Their Personal Data

By Joshua Brustein

Feb. 12, 2012

Facebook's pending initial public offering gives credence to the argument that personal data is the oil of the digital age. The company was built on a formula common to the technology industry: offer people a service, collect information about them as they use that service and use that information to sell advertising.

People have been willing to give away their data while the companies make money. But there is some momentum for the idea that personal data could function as a kind of online currency, to be cashed in directly or exchanged for other items of value. A number of start-ups allow people to take control — and perhaps profit from — the digital trails that they leave on the Internet.

"That marketplace does not exist right now, because consumers are not in on the game," said Shane Green, who founded a company called Personal in 2009.

The idea behind Mr. Green's company involves two steps. First, his team created a series of personal data vaults, which contain thousands of data points about its users (the company calls them owners). This data can be as prosaic as birth dates, or as specific as someone's preference for spicy foods. People control what information they share and remove data they don't want to share at any time.

The problem is that companies don't need to pay for the information when they get it free.

"The killer app isn't here yet," said William Hoffman, who is working on a multiyear study of the economics of personal data for the World Economic Forum. But with increased consumer awareness of the value of that information — Facebook could be worth as much as $100 billion — that may soon change. "I'm willing to bet that within the next 12 months something big will catch on," he said.

Shane Green, standing, founded Personal, a company that helps people control their personal data on the Internet, using what is known as a data locker. Daniel Rosenbaum for The New York Times

The concept of treating data like currency has long excited certain computer programmers and academics. But to almost everyone else, it is boring. Personal data management has none of the obvious appeal of social networks or smartphones. But concerns about privacy may be changing that, Mr. Hoffman said.

Many of the new ideas center on a concept known as the personal data locker. People keep a single account with information about themselves. Businesses would pay for this data because it allows them to offer personalized products and advertising. And because people retain control over the data in their lockers, they can demand something of value in return. Maybe a discounted vacation, or a cash payment.

Proponents of personal data lockers do not see them simply as a solution to privacy concerns. Rather, they hope that people will share even more data if there is a market for them to benefit from it.

The first step seems to be establishing trust. Reputation.com monitors the Internet for potentially harmful information and tries to remove it, while the Locker Project looks to create a single place where users can find what they see and do online. On Connect.me, which is in a private testing period, users vouch for one another, confirming that, for instance, someone is indeed a basketball player or a bookworm in an attempt to create a credible online reputation.

Let Us Help You Protect Your Digital Life

- With Apple's latest mobile software update, we can decide whether apps monitor and share our activities with others. Here's what to know.

- A little maintenance on your devices and accounts can go a long way in maintaining your security against outside parties' unwanted attempts to access your data. Here's a guide to the few simple changes you can make to protect yourself and your information online.

- Ever considered a password manager? You should.

- There are also many ways to brush away the tracks you leave on the internet.

To popularize the concept of the data locker, Personal wants to create a market for exchanging access to data. Mr. Green says users will reap either cash or other benefits, like heavy discounts on certain products. In January the White House announced that it would work with Personal and several other companies to allow students to download their academic data from federal databases and store it in a data locker. Personal says it is also working on partnerships with businesses.

A challenge for the company will be whether it can offer enough money to persuade people to use the system. Consumer information is worth billions in aggregate, but individually, the bits of data are worth practically nothing. A study by JPMorgan Chase last year showed that a unique user was worth $4 to Facebook and $24 to Google. Others looked at Facebook's recent filings with the Securities and Exchange Commission and placed the value of a user as high as $120.

The data that people store in their locker can be as prosaic as birth dates, or as specific as a preference for spicy foods.

Singly, a similar service that is still in a testing period, feels that developers can create better personalized services for people if all of the personal data can be accessed from a single location. With a person's permission, Singly draws data about them from around the Web, and allows them to share it with developers.

Jason Cavnar, a founder of Singly, is skeptical that personal data will be exchanged in the straightforward transactions that other data locker companies propose. While people may be willing to share their lists of Facebook friends, the bar is set higher for, say, the specifics of their financial history. Developers can build dozens of apps based on what one's friends on social media like to eat, but they are not churning out nearly so many that rely on, say, private financial data.

Instead, he says people will create data lockers and share their contents because they will receive compelling services by doing so. This idea has already been successful with Mint.com, which has shown that people will share confidential financial information in exchange for money-management advice.

People will not share information without a level of trust, and that is what the personal data management companies are trying to sell. The final barrier is that people may find creating detailed databases about themselves too onerous to justify the potential rewards. In order to create a real market for data, enough people need to see an immediate, tangible benefit in filling up their lockers, said Mr. Green of Personal.

He said he took note of this while presenting his product to groups of potential users. They nodded along with him as he told them about privacy and control. But when he showed his audience how entering their data into Personal allowed them to fill out online forms with a single click, something snapped for them.

"I don't think we quite realized how much of an emotional vein that tapped into," he said, "It's not easy to make data sexy or fun. It's not sharing photos with your friends on Facebook."

Exhibit O

Study on monetising privacy

An economic model for pricing personal information

[Deliverable – 2012-02-27]

II

Study on monetising privacy

An economic model for pricing personal information

Contributors to this report

Authors:
- Dr Nicola Jentzsch, DIW Berlin (Germany), team leader
- Sören Preibusch, University of Cambridge (United Kingdom)
- Andreas Harasser, DIW Berlin (Germany)

Advisers to the project:
- Professor Pio Baake, DIW Berlin (Germany)
- Professor Dorothea Kübler, WZB (Germany)
- Professor Sudipta Sarangi, Louisiana State University (U.S.A.)

ENISA project management:
- Demosthenes Ikonomou, ENISA
- Rodica Tirtea, ENISA

Other ENISA staff involved in the project:
- Barbara Daskala, Stefan Schiffner

Acknowledgements

Study on monetising privacy

An economic model for pricing personal information

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact details

For contacting ENISA or for general enquiries, please use the following details:
- E-mail: sta@enisa.europa.eu
- Internet: http://www.enisa.europa.eu

For questions related to this project, please use the following details:
- E-mail: sta@enisa.europa.eu

IV

Study on monetising privacy

An economic model for pricing personal information

Table of contents

Study on monetising privacy

An economic model for pricing personal information

Study on monetising privacy

An economic model for pricing personal information

List of tables and figures

1   Executive summary

Personal data is nowadays traded like other commodities in the market place, yet our understanding of cost–benefit trade-offs that individuals undertake when making purchases on the Internet and disclosing personal data is far from complete. This study analyses the monetisation of privacy. 'Monetising privacy' refers to a consumer's decision of disclosure or non-disclosure of personal data in relation to a purchase transaction.

Privacy is a human right; thinking about the economics of privacy does not change this basic fact. The authors of this report consider an economic analysis of privacy as complementary to the legal analysis as it improves our understanding of human decision-making with respect to personal data.

Do some customers of online services pay for privacy? Do some individuals value their privacy enough to pay a mark-up to an online service provider who protects their information better? How is this related to personalisation of services? The main goal of this report is to enable a better understanding of the interaction of personalisation, privacy concerns and competition between online service providers.

Consumers benefit from personalisation of products on the one hand, but might be locked in to services on the other. Moreover, personalisation also bears a privacy risk, i.e. that data may be compromised once disclosed to a service provider.

This report employs different methods in order to analyse the questions above. A theoretical model is introduced that takes into account the competition between two service providers. In this respect, consumers may select the service provider of their choice, depending on their privacy concerns and the offers made by service providers. In a variation of the model, consumers may select a service provider, but they may also choose whether they would like to have their services personalised in the future. The analysis of the data requirement of service providers and their pricing strategies shows that different data requirements serve as a differentiation device by which the providers may alter their prices/offerings.

A simplified version of the model was implemented in the laboratory in order to better understand how consumers make choices on the basis of the above-mentioned criteria. With 443 participants, the experiment is the largest laboratory experiment in the field of privacy economics to date. Different scenarios were implemented (so-called treatments), where participants were faced with two different service providers offering cinema tickets. The majority of participants who purchased two tickets in the laboratory experiment *remained loyal* to the service provider used for the first purchase (142 of 152 participants).

The laboratory experiment also shows that the majority of consumers buy from a more privacy-invasive provider if the service provider charges a lower price. A non-negligible proportion of the experiment's participants (13–83%), however, *chose to pay a 'premium' for privacy*. They did so in order to avoid disclosure of more personal data or because the privacy-friendly service provider promised not to use their data for marketing purposes.

2

Study on monetising privacy

An economic model for pricing personal information

The laboratory experiment was complemented by a hybrid and field experiment with over 2,300 participants and 139 transactions and observations. The field experiment confirmed the trends observed in the laboratory; the only difference noticed is that in case of no price difference the privacy-friendly service providers which request less personal data obtained a greater market share.

The report concludes with recommendations derived from this study. Users should be provided with options that allow them to disclose less personal data. Since such differentiation might lead to higher service prices, the EU regulatory framework should be sufficiently flexible to allow differentiation between service providers, enabling comparison of prices and requiring market players to offer privacy-friendly services.

In the future, easy-to-understand comparison of the data protection practices of service providers will become more important. Only if information practices (i.e. the collection and use of personal data) are more easily comparable will they play a useful role in the consumer's decisions.

Finally, portability of profiles for consumers will reduce potential switching costs which may arise if consumers choose to personalise their product at a particular service provider. Such profile portability should be conditioned on the consent of the consumer.

2   Introduction

2.1   Context and scope

The advances in Information and Communication Technologies (ICTs), the spread of the Internet and new business models, including social networks, as well as new practices such as behavioural profiling, web and location tracking (ENISA 2011a) are posing challenges[1] and are motivating the reform of the data protection legal framework in Europe.[2]

In a 2011 EuroBarometer Survey,[3] 74% of Europeans stated that they see disclosing personal data as an increasing part of modern life and 43% of Internet users say they have been asked for more data than necessary when trying to obtain access to or use an online service. A better understanding is needed of the basic mechanisms of consumers' data disclosure given their existing privacy concerns. Therefore, the rationale of this report is to better understand the consumers' trade-offs with respect to monetising personal information by disclosure or non-disclosure of it to a service provider (ENISA 2011a: 25). *Our knowledge about the economics of privacy; that is, the cost–benefit trade-offs individuals undertake when conducting economic transactions that involve personal information, is far from complete.* Likewise, more understanding is required to address questions such as whether and how service providers can gain a competitive advantage by collecting less information on consumers.

In its Communication on the Digital Agenda for Europe[4] the European Commission states that a lack of trust in the online environment is hampering the development of Europe's online economy and that consumers will not shop online if they do not feel their rights are clear and protected.

Personal data is nowadays traded among service providers like other commodities, meriting an analysis of individual transactions in the market place. For example, according to ENISA (2011b: 26–27), 47% of the service providers interviewed treated personal data as a commercial asset; and 48% revealed that they share data with third parties (ENISA 2011b: 26–27).

Therefore, it is important to also understand the economic dimension of privacy.

---

[1] *Reding, V. (2011), The reform of the EU Data Protection Directive: the impact on business, European Business Summit, Speech/11/349; Hustinx, P. (2011), Opening Session: 'General context – where we are now and where we are heading – current and future dilemmas of privacy protection', International Data Protection Conference, Hungarian Presidency, Budapest, 16 June 2011, pp. 7–8.*

[2] *European Commission, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 25 January 2012, available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[3] *Eurobarometer (2011), Attitudes on Data Protection and Electronic Identity in the European Union, SPECIAL EUROBAROMETER 359, available at:* http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

[4] *European Commission (2010), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions – A Digital Agenda for Europe COM(2010) 245, Brussels, 19.05.2010.*

2.2   Methodology, experiments and assumptions

In the first stage of this project the authors reviewed the literature on the economics of privacy, focusing in particular on economic experiments. A number of references are provided and discussed in section 4. One of the main findings is that a large share of literature is devoted to social exchange (such as surveys) and that economic experiments that implement real purchase transactions are rather scarce.

To the knowledge of the authors, there are no works in economics that *combine theoretical and experimental methods* for the analysis of the interplay of privacy concerns, product personalisation and competition. Identification of individuals is a precondition for the collection of their personal data and it is therefore also a precondition for personalisation. Personalisation is the tailoring of characteristics of a product or service to an individual consumer's preferences. Personal information as a base for personalisation allows the differentiation of consumers and dynamic price discrimination.

Personalisation can increase switching costs, if consumers who want to switch to a rival of their current service provider cannot simply transfer information from the old to the new provider. Disclosure of personal data might also induce privacy concerns for some individuals; this may limit the number of service providers to which the individual wants to disclose personal data.

For this study an economic model has been developed assuming competition between two service providers. The model developed and used in the study assumes an environment with differentiated products, i.e. differentiation in price, in personalisation level and/or personal data required. The model provides, on the one hand, insights into service providers' behaviour with regard to the collection of personal data on consumers in a competitive environment, and, on the other hand, information on how consumers react to the collection of such data. The model is presented in two versions – (a) a one-period version, which is used to illustrate some of the effects in the most basic setup where consumers make just one purchase; and (b) a two-period version including product personalisation and consumer 'lock-in', where consumers repeatedly interact with the service providers. The models used, the assumptions and the different scenarios are introduced in section 5 and the mathematical background is presented in the Annex.

To validate the model, different types of experiments have been conducted: the laboratory experiment, and a hybrid and field experiment (section 6). These are complementary to each other.

The laboratory experiment is a controlled environment, where the participants (in this study, students at a university in Berlin) know that they are part of an experiment. Laboratory experiments are widely used in economics for the analysis of economic incentives and decisions of individuals by involving them in real tasks and actions. Moreover, they can be used to test theories or the assumptions of theories. The actions of individuals do have real monetary and information implications for the individuals, which makes this research different from survey-based research.

5

At the end of the laboratory experiment, the participants filled out an *exit questionnaire* covering questions regarding privacy concerns and interest in personal data protection.

The hybrid experiment is a combination of laboratory and field, because we invited students from the experimental pool to a website on the Internet, where they could carry out a purchase transaction. Finally, in the field the participants (who come from the Internet-using population) do not know that they are part of an experiment. The websites used for the hybrid and field experiment are the same as for the laboratory experiment, with the only difference being the graphical design to make it more attractive for field visitors.

Theoretical as well as experimental methods have their limitations and rely on a few key assumptions. To reduce the complexity of the model, a number of simplifications were introduced, i.e. only two types of consumers were assumed, those with low and those with high privacy concerns. Regarding service providers, only two different types of requirements were assumed regarding the amount of personal data collected.[5] This was implemented in the experiment, however, without introducing strategic behaviour of service providers. The latter would have created problems from a data protection perspective and would have needed to be tested in separate experiments. Finally, the participants in the laboratory experiment were students at a large German university; this is a non-random selection and generalising the results to other populations and other types of transactions should be done with caution. Future research should use experimental methods to further expand to other types of transactions such as social networks.

2.3   Some findings

The answers that participants provided in the exit questionnaire with regard to privacy concerns and interest in personal data protection by organisations showed a rather high concern for privacy as well as a high interest in the topic (section 6.3.1).

Some other findings:
-   Almost all participants in laboratory experiment (over 90%) stayed with the service provider they first selected in case of two purchases;
-   If the price is the same at the two providers, the majority of purchases in the laboratory are conducted at the privacy-friendly online service provider (about 83% of all tickets sold); this observation shows that if offers are placed next to each other and consumers can compare the amount of data collected, consumers take information practice into account;
-   In the cases where also the price differs, the market share of the privacy-friendly service provider drops, below or close to one third.

When comparing the treatments in the laboratory and the field for all purchases, is noticeable that the privacy-friendly service provider has a much larger market share, if the differences in

---

[5] *A study published by ENISA in 2012 shows that the practice regarding data collection and how the principle of minimal disclosure is understood differs for the same type of service provided across Member States. See 'Study on data collection and storage in the EU', available on the ENISA web page:* http://www.enisa.europa.eu/act/it/library/deliverables/data-collection *.*

data collection are obvious and prices are the same. However, once prices change and a privacy-unfriendly competitor charges a lower price the privacy-friendly service provider loses market share. However, about a third of purchases of consumers show that are willing to pay a mark-up at the privacy-friendly service provider.

2.4 Structure of the study

This report is structured as follows. **Section 2** provides an introduction. **Section 3** covers the fundamentals of the economics of privacy, which are important for its economic analysis. **Section 4** provides an overview of the recent theoretical and experimental research in economics on personalisation, behaviour-based pricing and privacy.

In **section 5** an introduction to the economic model is provided. The details of this model are given in the **Annex** (section 10). **Section 6** provides an overview of the experimental work, which tests some of the assumptions and scenarios considered in the model. Finally, in **section 7** conclusions are drawn and recommendations made. The report is accompanied by a glossary of terminology.

Study on monetising privacy

An economic model for pricing personal information

enisa
European Network
and Information
Security Agency

7

3   The fundamentals of the economics of privacy

The economics of privacy is a field of research at the intersection of economics, law and computer science. It is devoted to the study of the economic cost–benefit trade-offs individuals undertake when disclosing personal data in economic transactions (so-called 'privacy calculus') as well as the competitive implications of protection of personal data for service providers.[6] In the following, however the focus is on the demand-side, i.e. the consumers. Two different types of exchanges are differentiated in the report to achieve a better classification of exchange models observable. Another basic taxonomy of online Service Models with a baseline differentiation into commercial and non-commercial can be found in ENISA (2011b: 11).

3.1   *Identification and personal information*

Identification is the process whereby a subject,[7] for example a natural person, is singled out from an anonymous mass, the so-called 'anonymity set'.[8] Identification can occur with different degrees, where higher degrees denote a more precise identification. Identification as differentiation may occur on the basis of personal information[9] such as name, address, identity numbers, behavioural and/or biometric data. The European Data Protection Directive applies four key elements to the definition of personal data, stating that personal data is (1) any information that is (2) relating (linked) to an (3) identifiable or identified (4) natural person.[10]

In the context of this report, we distinguish between personal information and private information as used in economics. *Personal information* contains differentiation power, because it singles a person out from the mass. *Private information,* on the other hand, denotes an unequal distribution of information among market players (e.g. consumers and firms), where one player has the information and the other does not. Therefore, information is private if it is not common (public) knowledge.[11] Personal data can be public, such as the names and birth dates of celebrities, yet it retains its differentiation power. However, personal information can also be private, for example if an individual manages to keep their real name and birth date private by using a false name and fictitious birthday.

---

[6] *An overview of the development of the field is presented in Acquisti (2010), Hui and Png (2006) and Jentzsch (2007).*

[7] *The precise description is 'personal identification', i.e. the identification of a natural person based upon that person's identifiers. Other types of identification might be possible, but are not relevant in the context here, such as pseudonymisation. Therefore, we will use 'identification' synonymously with 'personal identification'.*

[8] *Pfitzman and Köhntopp (2000).*

[9] *We use the expression 'personal information' interchangeably with 'personal data'.*

[10] *For an in-depth discussion see Article 29 Data Protection Working Party (2007). Opinion 4/2007 on the concept of personal data, adopted on 20 June, 01248/07/EN WP 136. As stated, we use 'personal data' and 'personal information' interchangeably.*

[11] *See Akerlof (1970).*

From the economic point of view as employed in this report, the state of privacy arises with asymmetric distribution of personal data between market participants, where one side *privately* holds personal information. Note that we do not suggest this as general definition, but rather as a definition employed in this report. Privacy is therefore a relationship of asymmetric distribution of personal data between market players. Many other definitions of privacy originate in the legal, political and philosophical disciplines.[12] The economic view does not devalue these concepts, but is complementary to them.

There are situations of *symmetric* and *asymmetric identification*. Symmetric identification occurs where both market sides can identify each other; in the asymmetric situation only one side can identify the other, not vice versa. Reciprocity in identification is an important ingredient for trust and can influence an individual's actions (see also section on 'Experiments with Identification'). Identification may or may not be subject to negotiation in economic transactions (Preibusch 2006). If the transaction is a take-it-or-leave-it offer conditioned on identification, consumers have no choice but to opt out completely. This means a potential customer does not buy the product or service.

If identification is not a component of the negotiations, challenges arise regarding the optimal level of identification. Identification differs among different types of transactions. While 90% of online shoppers state that they have disclosed their name and 89% their address for online shopping (Special EuroBarometer 2011: 40); among people using social networks, 79% state that they disclosed their name and 39% their home address when using social networks. Online purchases are often conditioned on identification. This is different for social networks, where truthful disclosure of identity data can be voluntarily chosen.[13]

3.2 Economic exchange of personal data

At the most basic level, we consider *economic exchange* as exchange intermediated by money. It should be differentiated from *social exchange* based on either real or perceived reciprocity between transaction partners. It is important to understand these concepts in order to understand the focus of this study. Social exchange, where consumers disclose personal data to firms in exchange for using their unpaid services, is not considered here. This would involve use of social networks or online services that are 'for free', except the consumer is monitored while using them (Internet search engines, free email services, etc.). We exclude *social exchange* and focus on transactions that are intermediated by money. In the transaction the consumer trades off monetary wealth and privacy.[14] Two different types of exchanges can be differentiated: (1) pure information transactions; and (2) composite transactions involving goods/services and information as a by-product (see Figure 1).

---

[12] *See for an example the Stanford Encyclopedia of Philosophy (2006). Privacy,* http://plato.stanford.edu/entries/privacy/

[13] *Google+ tried to implement a mechanism where users needed to identify themselves with their real name, but this met resistance from users; see TAZ (2011). Sag mir wer du bist, www.taz.de/!74756/.*

[14] *This is based upon Levitt and List (2007) regarding trading off morality and wealth.*

Study on monetising privacy

An economic model for pricing personal information

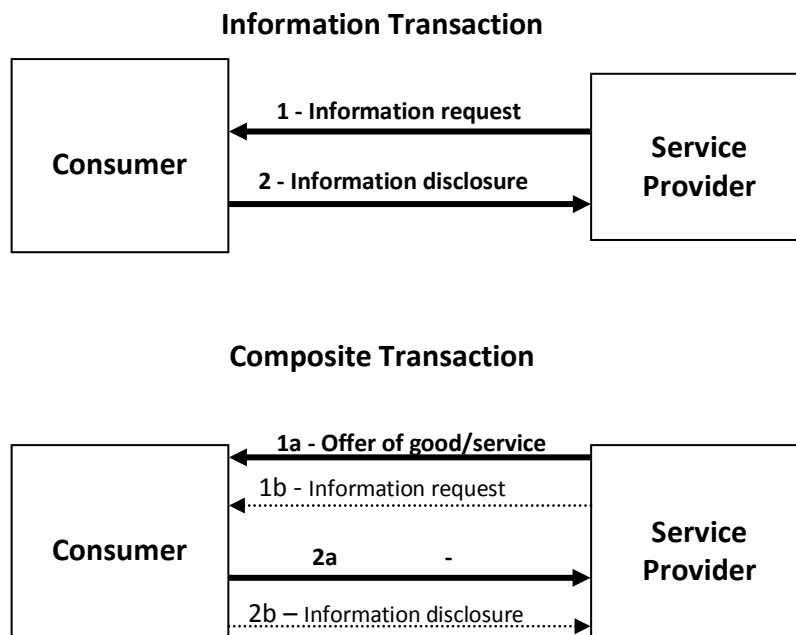**Information Transaction**

Composite Transaction

Figure 1 Information and composite transactions

In the **pure information transaction** (see upper part of Figure 1) consumers disclose personal data in the transaction. For example, consumers who participate in a survey disclose personal information.[15] A pure information transaction, which does not involve a physical product, allows the consumer to focus on the *terms of trade* (TOT) for personal data. Pure information transactions are not analysed in this report, because they involve different trade-offs and motivations. However, this is a topic for further research in future, requiring a social exchange analysis.

The second type of transaction displayed in Figure 1 (lower part) is a **composite transaction**, which involves a good or service and information as *by-product*. The main focus of the consumer is on the good or service the consumer wants to purchase. The exchange of personal data can be implied in the transaction[16] or be a by-product of it, where a person needs to disclose personal data actively. We lump these two versions of the composite exchange together under the term 'by-product'. Consider Internet shopping for music CDs: browsing behaviour and purchase actions of a customer are recorded by the firm and this

---

[15] *In many surveys consumers are not identified – they can provide information under conditions of anonymity. This is very different from the transactions analysed in this report.*
[16] *'Implied' means that the purchase itself already reveals preferences of the consumer and therefore personal information, if the consumer is identified.*

might go unnoticed by the consumer. However, if the consumer wants to have the CD shipped to his/her home address, this address needs to be disclosed.

A composite transaction is more complex when compared to a pure information transaction. A composite transaction requires greater cognitive processing ('thinking'), because the TOT for the good's purchase aside, there are also TOT for the information disclosure. The consumer has to weight (a) the costs and benefits of obtaining the good; **and** (b) the costs and benefits of information disclosure.

Note: It is important to separate the different types of transactions, because they entail different incentives and motives. At the most basic level, there is economic and social exchange. Transactions can be classified into pure information transactions or composite transactions involving goods/services and information, which gives rise to salience.

This brings us to another important concept: *salience* (DellaVigna 2009). Salience is 'relevance' or 'attention': if a feature of a product or service is salient, it stands out. Consider again the purchase of a CD on the Internet. While one firm might hide the terms of the privacy policy somewhere under the general commercial clauses, another might state directly, right next to the CD, that purchase will be recorded and purchase information shared with third parties. In this case, the terms of the policy stand out. More simply stated, consider a *composite transaction T* involving the *transaction of a good* (GT) and the *transaction of information* (IT):

$$T = GT + IT \qquad\qquad (1.1)$$

With salience included in (1.1) above,

$$T = GT + (1 - \lambda)IT \qquad\qquad (1.2)$$

The salience parameter λ, with $0 < \lambda < 1$, decreases the weight of IT in the composite transaction. $\lambda = 0$, on the other hand, denotes equal weight in attention devoted to the information and the good. Consider the example where a consumer compares offers for car insurance on the Internet. She will look for the best insurance at the lowest price. Privacy policy terms in the insurance contract are often not as important (i.e. they have low salience) as other product features. They may enter the consumer's cost–benefit trade-off concerning insurance with little or no weight in the decision.[17] The reason is that the primary purchase of car insurance is already highly complex. In Figure 1 (lower part) the bold print and arrows denote the consumer's focus. Composite transactions involve a privacy risk, i.e. a probability that personal data are compromised. It depends on the consumer's *privacy concern* or awareness and interest in data protection issues, whether the terms of the privacy policy are important or not in her decision.

---

[17] *In fact, privacy terms can bear additional costs for consumers by adding additional complexity to product comparisons. Individuals may then resort to external cues or heuristics in their decision-making.*

3.3 Truthful disclosure of personal information

Much theoretical work in economics is devoted to finding incentive-compatible mechanisms, which ensure that individuals reveal their true valuation of a good or service. The true valuation is private information held by the individual. In economics, if the revelation of truthful information is optimal for an individual, the mechanism of revelation is said to be 'incentive-compatible'. If a market mechanism is not incentive-compatible, individuals will reveal *some valuation*, but not necessarily their true one. Consider a situation where consumers are asked for personal data in order to obtain a discount. This personal data is their private information and there is no mechanism to verify whether the information they disclose is true. If consumers are *utility-maximising* and at the same time *concerned about their privacy*, it is a dominant strategy to lie to obtain the discount while cushioning the potential negative effects that arise from truthful disclosure of their personal data.[18,19] Individuals then resort to disclosing *some information*, which must not be related to their natural identity. Disclosing arbitrary information reduces differentiation power. Examples of such behaviour are the adoption of fake identities or pseudonyms in order to conceal the real identity (e.g. 'Donald Duck' instead of the real name). If differentiation power is reduced, privacy concerns fade away, which is problematic as they are at the very core of research in the economics of privacy. This is a lesson we learnt from the pilot conducted for this study: Here we observed individuals who strategically invalidated their personal data by disclosing obviously wrong information.[20]

Note: In order to protect their personal data, some individuals who are concerned with their privacy strategically invalidate their personal identifiers by disclosing bogus information. They have an incentive to do so given that the detection probability is low and the consequences of such information disclosure are not negative.

Much of the research screened for this study as potential literature background is not incentive-compatible, because the information disclosed by participants is not checked for accuracy. In particular, where individuals are asked for sensitive personal data that cannot be verified, results could be biased. Information that cannot be externally verified includes opinions, attitudes and norms, for example. However, a problem also arises where individuals are asked for verifiable data such as name, address, weight and height, but then this information is not verified. Thus, we classify research with no real economic/monetary

---

[18] *This explains why for incentive-compatibility it is not enough that a transaction is paid; rather, truthful revelation of private information must be the best response, no matter what other market players do; i.e. it must be optimal.*

[19] *This behaviour is common. In an anonymous representative survey conducted by BITKOM (2010) in Germany, almost every fourth Internet user stated that he/she has given false information on the Internet in the past. This amounts to about 12 million Germans. It is especially the name and age that are misrepresented, followed by telephone numbers, email addresses, income and to a lesser extent gender. In a recent Eurobarometer Survey it is reported that only 2 to 11% (depending on country) of Europeans provide false information (no context is given in the question); see Special Eurobarometer 359: 53; 135.*

[20] *For instance, the telephone number was indicated by '123456789'.*

12

enisa
European Network
and Information
Security Agency

Study on monetising privacy

An economic model for pricing personal information

component and no verification mechanism as 'not incentive-compatible' in the economic sense and exclude it from our literature review. This also excludes all studies that rely upon unpaid participation of individuals in surveys on privacy attitudes.

We also find that a pure information transaction is not comparable to a composite transaction, because a survey reply is $T = IT$ and social exchange, whereas an Internet purchase is $T = GT + (1 - \lambda)IT$ and economic exchange. In addition we excluded works with paid participation in surveys and studies that present participants with hypothetical choices, not involving any real actions and consequences. In hypothetical choice situation, respondents might not be able to tell how they would act or value a specific task/good in a hypothetical situation (Krahnen et al. 1997).

3.4 Privacy, personalisation and competition

To our knowledge, there are no works in economics that *combine theoretical and experimental methods* for the analysis of the interplay of privacy concerns, product personalisation and competition. *Identification is a precondition for the collection of personal data and therefore it is also a precondition for personalisation*. Personalisation is the tailoring of characteristics of a product or service to an individual consumer's preferences (see also Glossary, section 8). The base for personalisation is personal information. It allows differentiation of consumers and dynamic price discrimination.

When disclosing personal data, consumers often incur costs such as typing effort or some other disclosure aversion. At the same time, personalisation might increase consumer utility, if the consumer obtains a more tailored product. Once the product better fits the personal preferences of the consumer, he/she might be less inclined to switch to another firm. This might be the case because disclosing personal information had costs and the firm can now offer a better product.

In this case, it could be that price differences must increase to induce switching of consumers to the rival, once the consumer obtained a personalised product. *Personalisation can increase switching costs*, if consumers who want to switch to a rival of their current service provider cannot simply transfer information from the old to the new provider.

Disclosure of personal data might also induce privacy concerns and for some individuals these might increase with the rise in the number of service providers to which personal data are disclosed. These people might opt to stay at one service provider.

Study on monetising privacy

An economic model for pricing personal information

13

4   Literature discussion

4.1   Microeconomic theory

4.1.1   Behaviour-based pricing and product personalization

In the area of personalisation and *behaviour-based pricing (BBP)*, theoretical research can be separated into monopoly and duopoly models. While personalisation is the tailoring of the product to a customer's preferences, behaviour-based pricing is the practice of basing the price upon a customer's past purchase history.[21] We identified nine papers that use monopoly models and 27 papers that use duopoly models, which are relevant for our study. In this report, we use a duopoly as the existence of a rival competitor that allows consumers to choose between offers. Such choice is not the case in a monopoly setting. Choice is at the same time a precondition for switching behaviour. Thus, our approach excludes all monopoly models.

Among duopoly models, the majority are devoted to BBP. A classic result from this literature is that once both firms set personalised prices, they face a 'Prisoner's dilemma' due to intensified localised competition (Villas-Boas 1999; Fudenberg and Villas-Boas 2006; Stole 2006). Firms can now identify their own customers (their 'strong market') as well as those of the rival ('weak market') and accordingly compete in prices. For several different reasons, behaviour-based price discrimination *is not the same* as product personalisation.[22] Similar to the Prisoner's dilemma result above is the market outcome if both firms start to personalise products and lose a degree of differentiation.[23] In this case both firms are worse off in the second period of the game compared to the situation where both only provide standard products.

Zhang (2011) combines BBP[24] and product personalisation in one model. This paper, however, does not include consumer privacy concerns arising from product personalisation. The most closely related work is a duopoly with product personalisation and heterogeneous consumers in terms of brand preferences and privacy concerns. We identified Lee et al. (2011) as such a work. The authors use a Hotelling model[25] of two firms, which may offer standard and personalised products with personalised prices. Firms face three different kinds of consumers: the 'unconcerned' who always share information, 'pragmatic' ones who only share if a firm adopts privacy protection, and fundamentalists who never share data. The game has three stages. In the first, the firms decide simultaneously on privacy protection, in the second they decide on the price of standardised products and in the third on the pricing of personalised

---

[21] *Firms can differentiate between new customers and existing customers, who purchased their product in the previous period.*

[22] *For a discussion, see Zhang (2011: 171).*

[23] *Differentiation occurs where one firm personalises the pr**o**duct and the other does not.*

[24] *Firms can differentiate between new and existing customers, who purchased their product in the previous period.*

[25] *The Hotelling model is explained in the Annex to this report.*

products. Finally the consumers make their choice. The authors show that privacy protection, in the case where only one firm adopts it, works as a competition-mitigating effect. The privacy-friendly firm can enlarge market share by inducing pragmatists to share personal information. From this expansion it can earn substantial profits rather than compete with the rival for the other consumers.

Innovation in Modelling. Our model differs from the above as it introduces a second period, where consumers are able to switch to the rival. This is different from Lee et al. (2011), where the consumer choice is the final stage. Moreover, unlike Lee et al. (2011) and Zhang (2011), we do not introduce personalised prices, but a discount for information disclosure which is the same for all customers. Moreover, we have switching costs for consumers who decide to have their information stored for future periods. In that sense our research is also related to literatures on customisation (Dewan et al. 2000), but these works in general do not formalise privacy concerns.

4.1.2 Theoretical welfare effects of privacy regulations

Another fruitful area of research is the theoretical welfare effects of privacy regulations. For example, such regulations could prevent firms from sharing information with third parties. No general conclusions on consumer welfare can be derived from this literature, because the welfare effects of the regulations depend on the peculiarities of the model. At the most general level, the literature can be differentiated into models that analyse endogenous privacy policies; that is, a firm's incentive to adopt a privacy policy (Calzolari and Pavan 2006; Akçura and Srinivasan 2005), a consumer's choice to adopt anonymisation technologies or otherwise avert identification by the firm (Acquisti and Varian 2005; Conitzer, Taylor and Wagman 2010) and the effects of exogenous privacy regimes. In the latter, an outside regulator imposes rules on the market. In order to limit the discussion, we only consider one model (Hermalin and Katz 2006). The interested reader is referred to models such as Dodds (2008), Kahn, McAndrews and Roberds (2000) and Taylor (2004).

Consider a situation where there are laws on data protection. These laws function as a commitment device: consumers can sue a firm in case of breaches of data protection. Further, companies cannot influence the legal framework and change the rules in the short term. Therefore, laws are not considered as endogenous, but as an exogenously given framework for economic action. Since the legal framework influences the incentives of players, it also has an effect on economic welfare and rent distribution among market participants. In Hermalin and Katz (2006), n firms post a menu of offers to a finite number of households. Households are of two types, either good or bad.[26] There is no intrinsic valuation of privacy in this model on the part of the households. Two cases are outlined: a situation where firms move first and a situation where households move first.

---

[26] *'Bad' simply denotes a least-favoured indicator variable associated with the households. This is experimentally implemented in Giannetti and Jentzsch (2011).*

Firms move first – There are two scenarios: the Recognition Regime and the Privacy Regime. (i) Recognition Regime: Here, the firms make an offer and can compel households to reveal an indicator variable. This variable is a signal of the households' private information; (ii) Privacy Regime: In this regime firms can be forced not to use the indicator variable. However, they can write incentive-compatible contracts. These assure truthful revelation of private information. This leads all good types to reveal themselves, leading to the automatic revelation of bad types at the same time.

Households move first – In this situation, households can decide whether to reveal information or not. The outcome is identical to the Privacy Regime above. Good types will reveal their information (assumed bad types cannot mimic them). The firm then builds a certain belief about those households that did not disclose information and makes two offers to both groups. The authors establish conditions under which the location of property rights to information (firm or household) does not matter, as incentives to disclose by good types will automatically also reveal bad types.

4.2 Experimental economics

The literature devoted to empirical evidence on privacy is very diverse. In order to limit the review for this report, we apply a rigid approach. Firstly, we review only papers with an economic experimental design. To be classified as such, the experiment must entail a ***real economic transaction*** inducing a real monetary or reputational impact for the participant. The experiment might be a lab or a field experiment. Therefore, we exclude any study that elicits privacy attitudes or data disclosure with no further action derived from information collection, except for the privacy research conducted with the information collected by the researcher. Experiments in which experimenters deceive participants are excluded as well. Most of these experiments cannot be considered incentive-compatible. From 31 papers reviewed in the area of privacy, 12 were classified as surveys and 19 as experiments. Among the latter there are five identification experiments and four papers devoted to privacy (Adar et al. 2005; Beresford et al. 2011; Tsai et al. 2009; Giannetti and Jentzsch 2011). We refer briefly to the identification experiments and then discuss the other works.

4.2.1 Experiments with personal identification

Standard experiments are conducted in anonymity. The reason is the fear on the part of the experimenters that interpersonal effects arising through identification might contaminate economic incentives. For example, through identification an implicit multi-stage game could arise, individuals leave the laboratory and are still identified by others outside of it.[27] However, identification has proven to be a powerful variable that has – once introduced properly in a controlled way – a powerful impact on economic actions. At times this powerful impact reaches the extent of reversing theoretically predicted results (Bohnet and Frey 1997 1999; Charness and Gneezy 2008; Jenni and Loewenstein 1997). For example, identification in

---

[27] *In our experiment, individuals are not identified to other participants, but to the firm they are trading with.*

Dictator games[28] leads to greater contribution to the partner compared to anonymous situations. In fact the variation in the amount of money the Dictator leaves on the table for the recipient is a function of the degree of anonymity (Hoffman et al. 1996). Another example of the powerful impact of personal identification is public good games. In these games, individuals can decide upon a contribution to a public good. Identification leads to greater contribution in these games, because the actions of participants change significantly with less anonymity (Levitt and List 2007). Personal identification, therefore, has an impact on an individual's economic actions. Much more research is needed in this area in future. In our experiment, we introduce privacy considerations. Our participants need to identify themselves with a 'portfolio of personal information' (their real name, date of birth, etc.). Unlike in the above literature, our participants are not identified to other participants in the lab, but identify themselves to the firm at which they purchase, once they choose to have their information stored on the purchase form.

4.2.2   Economic experiments on privacy

Experimental designs that implement real purchase transactions are scarce. To the knowledge of the authors, there are only Beresford et al. (2010), Tsai et al. (2010), Gideon et al. (2006) and Gianetti and Jentzsch (2011). Other works are either survey-based experiments or incentivised pure information transactions (see for example Huberman et al. 2005). Beresford et al. (2010) use a hybrid field experiment[29] to analyse the willingness to pay for privacy, where participants were given the choice of buying a DVD from one of two competing online stores. While these stores were identical, one required more sensitive personal data than the other. In the test treatment, when the DVDs were one Euro cheaper at the privacy-invasive firm, virtually all buyers chose the cheaper store. In the control treatment with identical prices, people did not systematically prefer the more privacy-friendly firm, but chose both firms equally often. Not studied in this experiment was the effect of privacy policies and data usage. The authors conclude from their research that individuals are not willing to pay one Euro for their privacy.

In the experimental design of Giannetti and Jentzsch (2011), participants are of two types in terms of results they achieve in a test; they are either above or below a median, mimicking 'good' and 'bad' types. They can purchase a voucher and reduce the price of it by disclosing their test result. During each period there is a specific probability that information gathered by the firm to which data was disclosed will be compromised. Such an incident can lead to the disclosure of the data to other participants. The purpose of this experiment is to learn about the participants' decision-making, when there is a probability that information is compromised.

---

[28] *In a Dictator game, the Dictator has the task of dividing a specific amount of money between him- or herself and a recipient.*
[29] *We call a hybrid those experiments that are (a) laboratory combined with a live website; or (b) field experiments combined with an invitation to students registered in a laboratory pool.*

In Tsai et al. (2010), participants in the laboratory experiment are offered two different items by several vendors that differ in their protection of personal data. The offered products were a pack of batteries or a sex toy.[30] The experiment had three components: an 'online' survey about privacy concerns, the shopping simulation, and an exit survey. The authors state that the informational and monetary payoffs were real. They set the experiment up in such a way that individuals could find their valuation of privacy by making comparisons of the price charged by protective merchants vis-à-vis non-protective ones. This is a one-shot situation (one purchase) compared to our two-purchase situation. The stimulus varied included a simple link to a privacy policy as currently encountered on the web; and a way of making it more salient by having the search engine presenting privacy icons. Participants had to use their credit card to make the purchase from a real merchant online. The authors find that when privacy policy information is displayed in a more salient way, participants take the privacy policy into account and tend to purchase from online retailers that score higher on the privacy protection index. In this case, they are even inclined to pay a premium for websites that protect their privacy better. For example, for the sex toy purchases, 'participants in the privacy information condition made significantly more purchases from the high privacy website (33.3%) than participants in the no privacy indicator condition' (Tsai et al. 2010: 26). The researchers conclude that consumers are willing to pay for privacy once presented with easier-to-digest information.

Gideon et al. (2006) presented laboratory participants with an engine for searching or selecting websites to purchase two products (a surge protector and a box of condoms). The participants were asked to first purchase the less sensitive product and then the more sensitive product using the 'Privacy Finder,' which displays privacy policies in a more salient way. The authors found that the 'Privacy Finder' had a significant impact on purchases made with respect to the privacy-sensitive purchase. This is similar to Tsai et al. (2010). It is dissimilar to our experiment, however, in that we hold salience constant by not varying privacy policies or displaying privacy seals. Moreover, we introduce repeated purchases and with it personalisation and switching possibilities.

---

[30] *The product is intended to evoke privacy concerns.*

18

Study on monetising privacy

An economic model for pricing personal information

5   The model

5.1   Assumptions

Firms.[31] The supply side of the market consists of two firms $j \in \{A, B\}$ located at opposing ends of the Hotelling[32] line of length 1.[33] Firm A is assumed to be placed at location 0 and firm B at location 1. The firms sell a homogeneous good in each period $t \in \{1, 2\}$ with production cost normalised to 0.[34] Moreover, the firms require consumers to pay a price $p_{j,t}$ and to provide either a small or large set of personal data $d_j \in \{\underline{d}, \overline{d}\}$.[35] In each period, each firm offers the good at a price/data requirement combination $(p_{j,t}, d_j)$, which we refer to as a 'bundle'. The firms receive some exogenous benefit from collecting data. We assume that firm j receives benefit *q>0* each time a consumer buys at firm j if $d_j = \overline{d}$.[36]

Consumers. Consumers are differentiated in their location. Each consumer has an address $i \in [0, 1]$, which means that there are infinitely many consumers with their mass normalised to 1. Additionally, consumers have an exogenously given concern θ_i for disclosing their personal information. This privacy concern (or interest in data protection) may either be high or low and is denoted by $\theta_i \in \{\underline{\theta}, \overline{\theta}\}$ with $\mu = \Pr(\theta_i = \overline{\theta})$.[37] In each period a consumer chooses a firm to buy from. Consumers have a homogeneous valuation for the good, which is denoted by *v* and assumed to be sufficiently large to guarantee participation. Consumers incur a transportation cost for buying the good, which is equal to the unit transportation cost *r* times the distance between their own and the firm's location. Additionally, consumers face costs for disclosing personal data, which is denoted by $c(\theta_i, d_j)$ with $c(\overline{\theta}, d_j) > c(\underline{\theta}, d_j)$ and $c(\theta_i, \overline{d}) > c(\theta_i, \underline{d})$. Highly concerned consumers have higher cost for any data requirement and higher data requirements imply higher cost for any type of consumer. Furthermore, we assume that $c(\overline{\theta}, \overline{d}) - c(\overline{\theta}, \underline{d}) > c(\underline{\theta}, \overline{d}) - c(\underline{\theta}, \underline{d})$, i.e. that the difference between costs from a low and high data requirement is higher for highly concerned consumers than for others.

---

[31] We use 'firms' to refer to service providers.
[32] This model is named after its inventor Harold Hotelling (1895–1973). It is used to analyse competition with differentiated products.
[33] Setting the degree of differentiation to 1 can be done without loss of generality and just gives some fixed degree of differentiation.
[34] In the one-period version of the model the subscript t is dropped from the notation.
[35] The assumption of high/low requirements is a simplification to keep the model aligned with the experiment. Also note that this choice is made for the entire game. This is due to the assumption that the data requirement is a technological specification of the firm's services, like a form, which cannot be changed between periods.
[36] One might think of q as being an exogenous price, which a firm receives for selling its consumers' profiles to a third party. It might also represent some other benefit, for instance in-house use for market research.
[37] This is a simplifying assumption as the true type-space may be much richer. However, it increases tractability of the model. As in the experiment, firms set one price for all consumers; therefore they would not be able to discriminate further.

In the two-period model we introduce the possibility of product personalisation: Consumers may choose to get an increased value from the product, if they buy from the same firm in both periods. Personalisation can be a pre-filled form or some other modification of the product based upon personal data the consumer provided. However, in order to receive this benefit consumers also incur some cost, which is thought of as cost from an increased data requirement in order to carry out the personalisation. Consumers decide at the end of the first period whether they want personalisation. This is implemented in the experiment as the decision to have information stored for a pre-filled form. The possibility to personalise the product not only increases the benefit to consumers, but also induces the possibility of consumer lock-in.[38] Consumers only receive the benefit if they stay with the same firm throughout the entire game. In terms of utility this translates into consumers being able to gain some exogenously given benefit b, which is homogeneous across consumers. The consumers' decision whether to have the product personalised is denoted by $\beta \in \{0,1\}$ and comes at the cost of $c(\theta_i, \beta)$ with the same assumptions as on the cost function as above.[39]

This means that in addition to disclosure consumers must – for personalisation to work – allow storage of their data, which is associated with higher costs for highly concerned customers.

5.2 Timing in the model

One-period model: The timing of the game is such that in the first period, firm *A* starts by choosing a data requirement and a price. Afterwards firm *B* observes these choices and makes its choices on data requirement and price. This sequence of decisions can be justified by the observation that a large retailer (e.g. Amazon) moves first, while other smaller retailers are able to observe prices and data policy of the large firm and react accordingly. Then the firms offer the chosen bundles to the consumers, who make their choices. At the end of the period all choices are observed and utilities and profits are realised.

Two-period model: In this model the first period is played as in the one-period model. At the end of the first period, however, consumers decide on personalisation. Then the second period starts. The data requirement choices are the same as in the previous period. This can be thought of as choice of a specific technology to which the firm is tied for the entire game.[40] Again, firms choose prices in a sequential way and reveal their bundles. Consumers make their choices after observing these bundles. At the end of the second period respective utilities and profits are realised.[41]

---

[38] For example a pre-filled form allows consumers to save on costs and time once they return to the same firm.

[39] Without loss of generality we make the simplifying assumption that $c(\theta_i, 0) = 0, \forall \theta$. This means consumers do not face any costs, if they choose not to have their product personalised.

[40] Take for instance an online retailer, who decides upon a certain online form, which has to be completed by all consumers in order to carry out a transaction. This form is considered to be constant across periods.

[41] Note that we do not assume a discount factor. This is done in order to avoid an additional variable, which may drive behaviour in the model. One could argue that in online market environments periods are sufficiently close to each other.

enisa
European Network
and Information
Security Agency

Study on monetising privacy

An economic model for pricing personal information

5.2.1   One-period model

In the one-period model, firms maximise the profit function:

$$\arg \max_{p_j, d_j} \Pi_j(\cdot) = n_j(p_j + \alpha(d_j)q)$$

where a firm's market share is denoted by n_j and $\alpha(d_j) \in \{0,1\}$ denotes the firm's decision whether to have a high or low data requirement. Thus, $\alpha(\bar{d}) = 1$ and $\alpha(\underline{d}) = 0$. We will write α_j for $\alpha(d_j)$.

Consumers maximise their utility by deciding which firm to buy from:

$$\arg \max_j u_i(\cdot) = v - p_j - r|j - i| - c(\theta_i, d_j)$$

To analyse the firms' pricing and data requirements decisions, we start with the case where consumers do not incur any transportation cost. This allows us to focus on the fact that different data requirements serve as differentiation devices, which softens price competition and thus increases the firms' profits. Furthermore, zero transportation costs mimic the online environment in which the experiment takes place, where differences in location or exogenous brand preferences are absent. On the experimental website, the firms' offers for tickets are placed right next to each other. This is comparable to price comparison machines on the Internet, where offers are put right next to each other. The impact of positive transportation cost is also analysed below.

5.2.1.1 Special version with transportation costs equal to zero

With zero transportation costs firms face full price competition as differentiation in terms of location becomes irrelevant to consumers. The only differentiation which is still available to firms is the choice of different data requirements. Consumer choices are determined by the difference in prices and costs the firms impose on consumers with their data requirements. Since costs are different for the two groups of consumers the market may be segmented along the privacy concern of consumers. This holds in asymmetric equilibria where firms differentiate in terms of their data requirement and equilibrium prices are such that only highly concerned consumers choose the firm with the low data requirement. We can in fact observe such a situation in the laboratory experiment.

While asymmetric equilibria lead to positive profits, they only exist if the firms' benefit q from collecting data is not extreme; that is, neither very high nor very low. For extreme values of q both firms choose either high data requirements (if q is very high) or low data requirements (if q is very low) and earn zero profits. The logic behind these results is that, because firm B is the second mover, it might always choose to undercut firm A in prices and also decide to take the same or a different data requirement. Firm A anticipating firm B's behaviour tries to set its own price and data requirement such that firm B acts in a way which leaves firm A with positive profits. However, such a strategy is not available to firm A if q is either very high or very low.

Study on monetising privacy

An economic model for pricing personal information

Case 1: Let us start with the assumption that $q \geq \Delta c(\bar{\theta})$.

With $q > \max\left(\Delta c(\bar{\theta}), \frac{1}{\mu}\left[\Delta c(\bar{\theta}) - (1-\mu)\Delta c(\underline{\theta})\right]\right)$ we have a symmetric equilibrium with $d_j^* = \bar{d}, \forall j$ and $p_A^* = p_B^* = -q$. Firms subsidise consumers and make zero profits.[42] This equilibrium is efficient since $q \geq \Delta c(\bar{\theta})$ implies that the gains from high data requirements are higher than consumers' cost. Efficiency thus requires that both firms choose $\bar{d}$.

With $\Delta c(\bar{\theta}) \leq q \leq \frac{1}{\mu}\left[\Delta c(\bar{\theta}) - (1-\mu)\Delta c(\underline{\theta})\right]$ firms play a market segmenting asymmetric equilibrium with $d_A^* = \underline{d}$ and $d_B^* = \bar{d}$. In this equilibrium consumers with $\theta_i = \bar{\theta}$ buy from firm A while others buy from firm B. For prices it holds that $p_B^* > p_A^*$. Note, however, that this equilibrium is inefficient as efficiency still requires that all consumers provide a large amount of personal data.

Case 2: Now, turn to the case that $q \in (\Delta c(\underline{\theta}), \Delta c(\bar{\theta}))$.

In this case we get two asymmetric equilibria with the firm, which chooses $d_j^* = \bar{d}$ attracting all consumers with $\theta_i = \underline{\theta}$. These equilibria are efficient as q only outweighs the increased cost for one group of consumers and firms make positive profits.

Case 3: The final case left is that $q \leq \Delta c(\underline{\theta})$.

If in addition $q \geq \frac{1}{1-\mu}\left[\mu\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right]$ holds, we again get an inefficient market segmentation in an asymmetric equilibrium with $d_A^* = \bar{d}$ and $d_B^* = \underline{d}$. Prices are now such that $p_A^* < p_B^*$ and profits are positive.

If $q < \min\left(\Delta c(\underline{\theta}), \frac{1}{1-\mu}\left[\mu\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right]\right)$, we get an efficient equilibrium with $d_j^* = \underline{d}, \forall j$ and $p_A^* = p_B^* = 0$. Firms make profits equal to zero.

Summarising the cases we get asymmetric equilibria with positive profits for intermediate values of q, which are efficient only if $q \in (\Delta c(\underline{\theta}), \Delta c(\bar{\theta}))$. For very high (low) values of q we get efficient symmetric equilibria with both firms choosing the high (low) data requirement. In the laboratory and field we test whether there is a significant share of consumers with a high privacy concern that choose a privacy-friendly firm, if both firms are differentiated from each other.

---

[42] *Subsidisation occurs when firms provide consumers with a platform where they can store information and earn money with it; see also Lohr, S. (2010), 'You Want My Personal Data? Reward Me for It', New York Times, 17 July 2010, https://www.nytimes.com/2010/07/18/business/18unboxed.html*

5.2.1.2 General version with positive transportation costs

We now solve a general version of the one-period model with positive transportation cost. The firms' pricing strategies now change drastically, because they are ex-ante differentiated. We solve the game by backward induction, starting with consumers' choices for given sets of data requirements and prices.

Solving for the critical consumer (denoted with superscript *c*), who is indifferent between the two firms *A* and *B*, depending on the type yields:

$$i^c(\theta_{i^c}) = \frac{1}{2} - \frac{p_A - p_B + c(\theta_{i^c}, d_A) - c(\theta_{i^c}, d_B)}{2r}$$

Market shares can now be denoted by:

$$n_j = \left| L(j) - (\mu i^c(\bar{\theta}) + (1-\mu)i^c(\underline{\theta})) \right|$$

with location $L(A) = 0$ and $L(B) = 1$.

Then solving for firm *B*'s reaction function in prices yields:

$$p_B^* = \frac{1}{2}(r + p_A + \mu(c(\bar{\theta}, d_A) - c(\bar{\theta}, d_B)) + (1-\mu)(c(\underline{\theta}, d_A) - c(\underline{\theta}, d_B)) - q\alpha_B)$$

The pricing function indicates the following:

- The higher the cost firm *B* imposes on consumers compared to the cost firm *A* imposes on them, the lower will be firm *B*'s price.
- Firm B's optimal prices increase, if the unit transportation cost *r* rises, as it becomes more costly to choose the firm which is located further away from one's own location.
- The decision to have a high data requirement and the pricing decisions are strategic substitutes. Thus, if firm *B* requires $\bar{d}$, p_B^* decreases.

Comparing profits under the two different data requirements leads to the following decision:

$$d_B^* = \begin{cases} \underline{d}, \text{if } \mu\Delta c(\bar{\theta}) + (1-\mu)\Delta c(\underline{\theta}) > q \\ \bar{d}, \text{otherwise} \end{cases}$$

Note that $\Delta c(\theta_i) = c(\theta_i, \bar{d}) - c(\theta_i, \underline{d})$ and thus firm *B*'s data requirement decision is independent of *A*'s data requirement.

In the next step, solving for *A*'s pricing function in general yields:

$$p_A^* = \frac{1}{2}(3r - \mu(c(\bar{\theta}, d_A) - c(\bar{\theta}, d_B)) - (1-\mu)(c(\underline{\theta}, d_A) - c(\underline{\theta}, d_B)) - q\alpha_A - q\alpha_B)$$

Under $\mu\Delta c(\bar{\theta}) + (1-\mu)\Delta c(\underline{\theta}) > q$ comparing *A*'s profits for the different data requirements leads to the following equilibrium:

$$(d_A^* = \underline{d}, p_A^* = \frac{3r}{2}), (d_B^* = \underline{d}, p_B^* = \frac{5r}{4})$$

If $\mu \Delta c(\overline{\theta}) + (1 - \mu) \Delta c(\underline{\theta}) < q$, the same comparison of profits leads to the equilibrium:

$$(d_A^* = \overline{d}, p_A^* = \frac{3r - 2q}{2}), (d_B^* = \overline{d}, p_B^* = \frac{5r - 4q}{4})$$

In both equilibria we obtain market shares of:

$$n_A^* = \frac{3}{8}, n_B^* = \frac{5}{8}$$

Note that both equilibria are symmetric and efficient in terms of comparing the benefits from high data requirements and the average cost for providing personal data. Symmetry comes from the fact that once a certain data choice is optimal for one of the firms it also has to be optimal for the other firm, as these choices balance the firms' benefits from high data requirements and the negative impact on their demand.

5.2.2   Two-period model

In this model consumers not only make a choice on the firm, but also whether to have personalisation or not. This leads to the following maximisation problem for the consumers:

$$\arg \max_{j_1, j_2, \beta} u_i(\cdot) = \sum_{t=1}^{2} (v - p_{j,t} - r|j - i| - c(\theta_i, d_j)) - c(\theta_i, \beta) + \psi \beta b$$

with $\beta = 1$ if the consumer opts for personalisation and $\beta = 0$ otherwise as well as $\psi = 1$ if $j_1 = j_2$, and $\psi = 0$ if $j_1 \neq j_2$, i.e. the benefit from personalisation b can only be received if the same firm is chosen in both periods. In the laboratory experiment, we call these buyers 'loyals'.

The firms' profit function is the sum of the firms' profits in both periods with consumers buying at price $p_{j,t}$ plus the exogenous benefit q if $d_j = \overline{d}$ for each consumer. Thus firms maximise:

$$\arg \max_{p_{j,1}, p_{j,2}, d_j} \Pi_j(\cdot) = \sum_{t=1}^{2} n_{j,t}\left(p_{j,t} + \alpha(d_j)q\right)$$

Again, it holds that $\alpha(d_j) \in \{0,1\}$ with $\alpha(\overline{d}) = 1$ and $\alpha(\underline{d}) = 0$ and we will write α_j for $\alpha(d_j)$.

The consumers' decisions to have their products personalised are influenced by a trade-off between the costs and benefits of personalisation. A consumer only chooses a personalised product if $c(\theta_i, 1) < b$. But as consumers can only realise the benefit under the condition that $j_1 = j_2$ rational expectations may lead them to strategically avoid personalisation in order to prevent being locked in in the second period.[43] This can be the case if, for instance, the price

---

[43] *We note that a more realistic assumption might be that consumers are not aware that personalisation can lead to lock-in. However, in the laboratory, most participants behaved rationally. We observed few switchers that stored their data, but still switched.*

differences are such that the firm charging a lower price in the first period charges a higher price in the second period. If the net difference is higher than the net benefit for the consumer, this consumer may choose not to have the product personalised although $c(\theta_i, 1) < b$. Due to this reason, there can be no equilibria in which consumers personalise and switch firms in the model.

Turning to the different cases and defining $\Delta b(\theta) = b - c(\theta, 1)$, we have to consider the following three scenarios (note that $c(\underline{\theta}, 1) \leq c(\overline{\theta}, 1)$ also implies $\Delta b(\underline{\theta}) > \Delta b(\overline{\theta})$):

a) No consumer chooses to get a personalised product: $0 > \Delta b(\underline{\theta}) > \Delta b(\overline{\theta})$

b) Only those with a low concern choose to personalise: $\Delta b(\underline{\theta}) > 0 > \Delta b(\overline{\theta})$ and do not switch

c) All consumers have their product personalised $\Delta b(\underline{\theta}) > \Delta b(\overline{\theta}) > 0$ and do not switch.

5.2.2.1 Special case with transportation costs equal to zero

Again, we start by considering the case with transportation cost of zero, which mimics the online environment of the experiment. Comparing the one- and two-period model and considering the impact of personalisation on the firms' decisions with respect to their data requirements, we have two counteracting effects. On the one hand firms have a higher incentive to differentiate their products by choosing different data requirements, which increases the parameter range, where inefficient equilibria exist. Only by differentiating are firms able to make positive profits in both periods.

On the other hand, personalisation abates this effect as it allows firms to make positive profits even if they choose the same data requirements. These profits require transferring surplus from consumers to the firm, but as the possibility of personalisation increases welfare, consumers may still be better off in equilibrium. To analyse these two effects we first consider the case in which no consumer opts for personalisation. The impact of personalisation is analysed in the next subsection, where we assume that only consumers with $\underline{\theta}$ have an incentive to opt for personalisation. In the following, we restrict the analysis to the case with no personalisation as well as the case with a share of consumers personalising.

5.2.2.1.1 No personalisation: $0 > \Delta b(\underline{\theta}) > \Delta b(\overline{\theta})$

The range of inefficient market segmentations, where consumers with a low (high) privacy concern choose the firm with the high (low) data requirement, increases in this scenario.[44] This is due to the fact that differentiating from the competitor becomes more attractive, as there is two times the surplus to be extracted from consumers, compared with the one-period model. Still, symmetric equilibria, which are efficient, exist if q is sufficiently high or low. In the first case it becomes too attractive to choose the high data requirement, while in the second case it becomes too prohibitive to impose high costs on consumers, so that firms

---

[44] A detailed formal analysis is provided in the appendix of this report.

rather refuse to differentiate. For intermediate values of *q* the asymmetric equilibria are efficient.

5.2.2.1.2 Personalisation with $\Delta b(\underline{\theta}) > 0 > \Delta b(\overline{\theta})$

We solve the model for different kinds of parameterisations. Starting with an intermediate value of $\mu = 1/2$, we derive several different kinds of equilibria. Similar to the case with $0 > \Delta b(\underline{\theta}) > \Delta b(\overline{\theta})$ these equilibria are symmetric for either high or low values of q. For intermediate values of q we get asymmetric equilibria. However, due to the lock-in effect even symmetric equilibria allow firms to make positive profits, as they are able to extract some surplus from their consumers, without losing too many of them to the competitor.

For other parameterisations, i.e. for $\Delta c(\overline{\theta}) = \frac{2}{3}$, $\Delta c(\underline{\theta}) = \frac{1}{3}$ and $\mu = \frac{1}{4}$ as well as $\mu = \frac{3}{4}$, we obtain the result that only asymmetric equilibria exist for a wide range of parameters *q* and *b*. In all cases except for one, Firm *A* chooses to be the firm with the high data requirement. Only in one case, where *q* is comparably low, does Firm *A* choose to be the firm with the low data requirement.[45] Firms' choices are simulated in the laboratory and field by implementing different situations, i.e. situations where firms are similar in their offers and situations where they differ on the data requirements. The experiment would otherwise have become too complicated, also from a data protection point of view.[46]

Comparing the firms' profits shows that Firm *B* may lose its second mover advantage, which is usually found in models where firms compete on prices and decide sequentially. This is due to the fact that in an equilibrium, where consumers are segmented, Firm *A* (being the first mover) is able to secure all consumers with a low concern. These consumers react more strongly to price increases, but as they are at the same time choosing to get their product personalised, they are also prone to lock-in. Therefore, firm *A* is able to extract more surplus from its consumers in the second period and thereby can gain higher overall profits under most parameterisations.

5.2.2.2 General version with positive transportation costs

Under the scenario that no consumer chooses to have the product personalised, we get a simple repetition of the pricing game. Thus, the equilibria are as in the one-period model with $p_{j,1}^* = p_{j,2}^*, \forall j$. In all cases where at least some of the consumers have an incentive to choose personalisation the solution of the second period requires solving the whole game. The reason is that consumers who choose to personalise base their decision of firm choice in the first period on the expected prices in the second period: with rational expectations no consumer who anticipates that it is optimal for him to buy from different firms would opt for

---

[45] *However, one may also be able to replicate the result of symmetric equilibria in case of extreme values of q, if less parameters were fixed.*

[46] *For example, we would have to introduce strategic players (participants) that act as firms. However, in an experiment with true personal data disclosed, we create additional data protection problems, if other participants (and not the experimenter) collect this information.*

enisa
European Network
and Information
Security Agency

Study on monetising privacy

An economic model for pricing personal information

personalisation. As along as consumers anticipate rather high price differences in the second period, avoidance of personalisation may be the optimal behaviour.[47] Moreover, as the fraction of consumers who opted for personalisation in the first period also determines the equilibrium prices in the second period, second-period prices and first-period decisions and demands are interdependent. The implied maximisation problem of the firms becomes rather complex; therefore we focus on the case with $\Delta b(\underline{\theta}) > 0 > \Delta b(\overline{\theta})$, as it features consumers who choose to personalise as well as those who refuse personalisation. Using the result from the one-period model with positive transportation costs, we also restrict the analysis to symmetric equilibria. As $r > 0$ already provides differentiation between firms, the differentiation tool of choosing different data requirements becomes obsolete. Thus, if it is beneficial for one of the firms to choose $d_j = \overline{d}$ it is also beneficial for the other. We still have two different scenarios as equilibrium candidates. The first is one where not all consumers with $\underline{\theta}$ opt for personalisation, but instead switch the firm they buy from. The second scenario is such that all consumers with $\underline{\theta}$ opt for personalisation and do not switch firms. Concerning the first candidate and taking into account equilibria with both interior and corner solutions for the firms' pricing decisions, we can show that no equilibrium exists where some of the consumers with $\underline{\theta}$ switch. With interior solutions the difference between firms' optimal prices is too low in order to compensate consumers for losing their personalisation benefit, which means that none of them would want to switch (the respective equilibrium does not exist). Considering corner solutions, where firms set the maximum price within certain intervals, all consumers would either choose Firm A or Firm B in the second period. However, the maximum prices, which allow for such a scenario, are also not part of an equilibrium, as it gives the firm which would be without consumers in the second period high incentives to marginally reduce its price in order to attract at least some consumers who did not personalise.

Turning to the second scenario, where all personalising consumers are loyal and focusing on interior equilibria in which both firms serve both types of consumers, the analysis shows that the firms' equilibrium profits do not depend on q or on b. These results resemble the results obtained in the one-period model. They are based upon the fact that the firms' pricing behaviour is driven by the marginal profits from attracting additional consumers. Moreover, analysing the firms' profits with respect to μ, i.e. the fraction of consumers who do not personalise, shows that the firms' profits are the higher the lower μ and thus the higher the number of personalising consumers. Intuitively, the more consumers that personalise the more consumers are locked in in the second period and the higher the firms' equilibrium prices and profits. A similar but more complex reasoning holds for the firms' pricing strategies in the first period. Although firms try to attract a high number of personalising consumers by charging low prices, firms also take into account that price competition in the second period

---

[47] *In order to focus on the differences in data requirements and prices in the experiment, we avoided prices changes from one period to the next. The participants were informed that prices remained constant. Note that in the laboratory the two-period model without transportation costs was implemented.*

Study on monetising privacy

An economic model for pricing personal information

tends to be less intense if the firms' market shares in the first period are rather symmetric. This holds especially for Firm B, which can anticipate that the price Firm A will choose in the second period is the higher the more personalising consumers Firm A has attracted in the first period. The last effect dominates the first and the firms' first-period equilibrium prices will be the higher the more consumers personalise. Summarising these results indicates that while the consumers' benefits from personalisation do not affect the firms' pricing strategies directly, personalisation induces different strategic effects, which soften price competition and lead to higher firms' profits.

The **Annex** contains the technical background of this model.

Study on monetising privacy

An economic model for pricing personal information

6   The privacy experiments

We now discuss the design, experimental protocol and results from the different types of experiments we conducted: the laboratory experiment, hybrid and field experiment. These are complementary to each other. The laboratory is a controlled environment, where the participants know that they are part of an experiment. Participants are students at a university in Berlin. The hybrid is a combination of laboratory and field, because we invited students from the experimental pool to a website on the Internet, where they could do a purchase transaction online without coming to the laboratory. Finally, in the field the participants do not know that they are part of an experiment and they must not be students, but come from the Internet-using population as a whole.

6.1   Translation of the model into the experiment

We implemented a simplified two-period version of the model without transportation costs. The implementation is described in detail below. In essence we tested the following aspects: whether there are different types of consumers with different privacy concerns, as well as their firm choice and switching behaviour. The following situations were implemented:

-   Two-period version of the model with zero transportation costs and with both firms choosing the same data requirements and prices. This version contains the personalisation option for consumers as well as constant prices;[48]
-   Two-period version with one firm choosing a low data requirement and the other a high data requirement either with or without price differences. This version also contains the personalisation option and constant prices.

There were two real private companies (Event Sales and Cine Sales) offering the tickets over the Internet. Their offers were placed right next to each other in order to obtain a scenario with no transportation costs. **Note that strategic firm behaviour as in the model was not implemented in the laboratory, because the firms were 'computerised'. Moreover, participants were informed that prices do not change across periods.** This restriction was implemented to preclude participants disclosing their personal data to other (human) participants, which could create severe data protection problems outside of the laboratory.

6.2   Laboratory experiment

Laboratory experiments are widely used in economics for the analysis of economic incentives and decisions of individuals by involving them in real tasks and actions. Moreover, they can be used to test theories or assumptions of theories. The actions of individuals do have real monetary and information implications for the individuals, which makes this research very different from survey-based research; see section 3 of this report.

---

[48] To enable a focus on and a testing of the reaction of consumers with respect to the difference in the data requirements **only**, we held the prices constant across periods. This was necessary in order to reduce the variation in stimuli.

6.2.1   Place, time period and participants

We conducted the experiment at the Technical University of Berlin in Berlin, Germany, between June and November 2011.[49] Altogether 443 students of different disciplines participated, which makes this experiment the largest laboratory experiment on the economics of privacy to date. The students who participated are registered in a student pool and they were invited to the lab sessions with a neutral email invitation. While they knew that they were participating in an experiment, they were aware that they were carrying out transactions on a live website on the Internet. They had no details about the ultimate purpose of the experiment and did not know that it was about personal data disclosure in particular.

6.2.2   Design of the laboratory experiment

The invitation was framed in a neutral way by referring to an economic experiment only. This way, we avoided pre-selection effects that might arise if the experiment only attracted individuals who were interested in privacy matters.[50] Participation was voluntary. After admission to the laboratory, the participants were given the instructions for the experiment. These instructions explained the rules of the experiment in simple terms. After signing the consent form to participate, each participant started the experiment by doing a brief comprehension test that allowed us to ensure that instructions were well understood by the students. Participants used a website in the laboratory that is similar to the field website. The website is an Internet portal of providers of cinema tickets. On this website, they could choose a cinema and showing and then purchase the ticket from one of the two firms providing the tickets (Figure 2 shows a screenshot from the field experiment, Table 1 shows the different treatments). The difference between the firms is described below. After the finalisation of the purchase, the participants could repeat the transaction if they wanted to buy a second ticket. Only the repetition ensures that we can observe switching behaviour and it ensures that we implement the two-period model.

Note: In the laboratory, hybrid and field, all components of the composite transaction were real, meaning the collection of personal data, the cinema tickets sold and the payment with the participants' own money. Participants were not deceived, either about the transaction, the firms, the data collection, or data usage.

Participants could compare the offers of the two firms and choose the offer they liked best or not purchase at all, because purchase was voluntary. We varied the differences between the two firms in order to extract the effects of one firm requesting more information than the other or the effect of different data usages. Regardless of the firm chosen, each purchase was subsidised by the experimenters by €2, resulting in residual prices as low as €3 per cinema ticket even for peak cinema times.

---

[49] *Two pilots were conducted, one in June and one in July. The main sessions then took place in August, September and November.*

[50] *This interest or motivation could be associated with experimental outcomes and therefore bias the results obtained in this study.*

Study on monetising privacy

An economic model for pricing personal information

Figure 2 Order summary and choice of firms

At the end of the experiment the participants filled out an exit questionnaire, paid the subsidised ticket price, obtained the ticket/s and left the laboratory. A show-up fee was paid out and set off against any outstanding payments for the purchases made. Individuals who did not purchase anything obtained only the show-up fee, as is common in experimental research. Note that the participants had to pay the outstanding balance with their own money. This way we avoided budget effects and 'gambling' arising from money given to the participants upfront, before the experiment took place.

In order to extract the effect that differences in data requirements between firms make on purchase behaviour, we varied the stimulus. The situations with a varied stimulus were then compared to a basic control treatment in which the firms are similar. Next, the difference between the offers of the two firms were either: (a) differences in number of data items required from the participant; (b) differences in data items required and differences in prices; (c) differences in data usage, while both firms have the same prices; and (d) differences in data usage and prices; see Table 1.

We conducted two pilot sessions with 48 participants aimed at testing the design. In the treatments with price difference and different number of items, the privacy-invasive firm

charged a ticket price €0.50 below its competitor.[51] The pilots showed that a €0.50 price difference leads to a noticeable variation in behaviour of the participants; they do not all choose the same firm, but vary in their choice.

Table 1 Variation in treatments

Treatment	Settings (Variations)
1	Difference in data usage
	Difference in prices
	Privacy policy exists at both firms
2	Difference in data usage
	Same prices
	Privacy policy exists at both firms
3	Difference in number of data items
	Difference in prices
	Privacy policy exists at both firms
4	Difference in number of data items
	Same prices
	Privacy policy exists at both firms
5	Same information items
	Same prices
	Privacy policy exists at both firms

In the basic control treatment (5 in Table 1), the firms are identical with regard to the prices and/or their data requirements. This is our benchmark scenario. In the other treatments, either the prices or the data requirements are varied. Note that prices remain constant from one period to the next in all treatments.

Difference in data requirements: Both firms in the experiment always asked for a minimum set of personal data such as full name, email address and date of birth. Depending on the treatment, the stimulus in data collection was either: (a) the collection of additional data items (such as mobile phone number) by the privacy-unfriendly firm; or (b) the usage of the email address for advertising at the privacy-unfriendly firm.

In order to create incentive compatibility, we implemented a 'lie detection device' that ensured truthful revelation of actual personal data by participants. While this can affect external validity, it ensures that individuals have a real privacy concern. As explained above, if participants have the opportunity to misstate personal information, they can cushion potentially negative effects arising from its disclosure. We introduced a mechanism in which we verified the students' personal data. Participants knew that once they provided wrong information their payoff would collapse to zero. Any incorrect personal data was detected

---

[51] We chose this to be below the 1 Euro price difference in Beresford et al. (2010).

enisa
European Network
and Information
Security Agency

Study on monetising privacy

An economic model for pricing personal information

with 100% probability, because the research assistants checked the data provided by all buyers in the laboratory.

6.3   Results from the laboratory experiment

As stated, there were 443 participants in the laboratory experiment including 24 participants in the second pilot, where we did identity verification.[52] Of these 443 people, 40.41% were women and 59.59% men. In the general population in Germany, there are 51% women and 49% men. However, in the German population there is a higher share of men (about 80%) who use the Internet, compared to 70% of women.[53]

Summary statistics: The purchase statistics are given in Table 2. Across the whole sample (n=443), 251 individuals did not buy any tickets, 40 bought only one and 152 bought two tickets, which is a relatively high share of two-time buyers (57%). Among those who bought two times, 142 (93.42%) stayed with the firm they had chosen in the first period and only 10 switched (6.58% of two-time buyers).[54] Therefore, by far the larger share remained with the same company. Note that this is the sample across all treatments, some of which have variations in prices or data requirements, although there is no variation over the two periods in those.

Furthermore, there is no significant difference in terms of privacy concern or interest in data protection between the buyers and non-buyers. This means that the purchase action does not seem to introduce a pre-selection effect in terms of attracting only individuals that have little to no privacy concern or little to no interest in data protection.[55]

In the analysis below, we disaggregate the different treatments, because these differences influence the decision of individuals in terms of which company they choose. Interestingly, there were 10 people who switched from one firm to another. Whereas 9 people switched from Firm 1 to Firm 2, one person switched from 2 to 1. Three of the 10 switchers did not store data and seven individuals stored data, but still switched to the other company in the second period to buy their tickets there. These people had to re-enter the information at the new company. Note that the instructions clearly explained to individuals that prices remained constant across periods. In the exit questionnaire, we could probe the reasons for switching. All switchers recognised that they had bought from different firms. Some mentioned that they randomised, because prices were the same; others wanted to try out the other firm. Therefore, there seems to be no systematic behavioural bias.

---

[52] We did two pilots for the experiment: one without identity verification and one with identity verification. Only data of the latter was included in the laboratory dataset.
[53] Initiative D21 e. V.; TNS Infratest (2008, 2011): (N)Onliner-Atlas.
[54] Those that stayed with the same firm were defined by us as 'loyals' and those two-time buyers that did not were defined as switchers. If we refer to both types of buyers (loyals and switchers), we refer to two-time buyers.
[55] We conducted the Mann-Whitney test on differences in medians as well as t-tests to analyse if there is a difference between the group of non-buyers and the group of buyers who bought at least one ticket in either period. The latter variable also included two-time buyers.

Study on monetising privacy

An economic model for pricing personal information

Table 2 Overview statistics (whole sample, all treatments)

Overview Statistics	Number	Percentage of total	Bought at Firm 1 (privacy-friendly)	Bought at Firm 2 (privacy-unfriendly)
Participants			(across periods, percentage of total)	
- Did not buy any ticket	251	56.66	-	-
- Bought one ticket	40	9.03	-	-
- Bought two tickets	152	34.31	-	-
Total	443	100.00		
Two-time buyers				
No. of two-time buyers	152			
- of which are loyal to same firm	142	93.42	59 (41.55%)	83 (58.45%)
* loyals who stored data			27 (45.76% of 59)	49 (59.04% of 83)
- of which are switchers	10	6.58	9 persons switched from Firm 1 to 2; one person switched from 2 to Firm 1	
Total	152	100.00		

6.3.1 Privacy concern and interest in data protection

In the questionnaire, we collected answers to a number of questions related to the participants' purchase experience, trust and risk perceptions as well as data protection. Moreover, we used the instrument developed in Smith et al. (1996) on measuring the privacy concern of individuals. The instrument is a battery of 15 questions, where answers are given on a Likert scale, ranging from 'strong disagreement' to 'strong agreement' with higher values denoting higher concern. We have calculated the average and median across individuals (see Figure 3 for the average).

This figure shows that the there is a high frequency of individuals (over 361 out of 443 participants) with an elevated privacy concern. Note that we posed these 15 questions in an exit questionnaire. When using data from the whole sample, the privacy concern (median) is weakly correlated with the choice of the firm in period 1 (Pearson coefficient 0.0953, p-value=0.0449). But the choice is not correlated with the average privacy concern.

Apart from the 15 questions used for calculating the privacy concern, we asked one additional question on the interest in the practices of organisations with regard to protecting personal data. The answers to this question were not used in the computation of the privacy concern.

34   enisa   *European Network   Study on monetising privacy
                  *and Information
                  *Security Agency   An economic model for pricing personal information

The overwhelming majority of participants in the laboratory experiment revealed that they are either 'interested' or 'very interested' in whether a firm protects their information (about 93%). Only about 0.7% of participants stated that they are 'not interested at all' if organizations that collect personal data also protect this information.
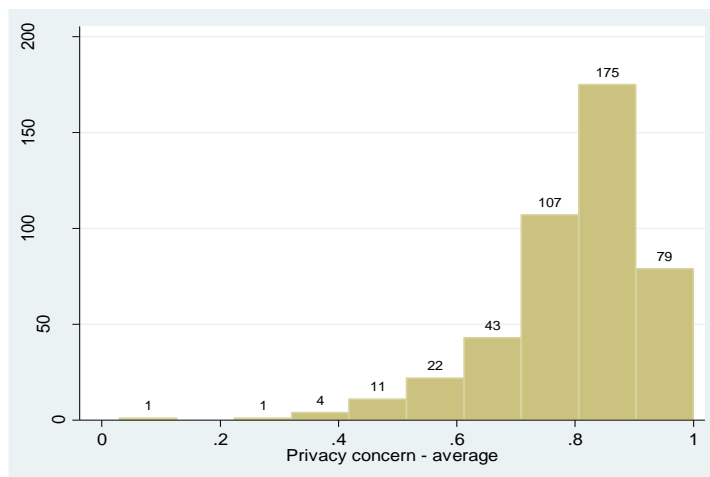

Figure 3 Privacy concern among participants

6.3.2   Monetising privacy

Do some people pay for privacy? Meaning, do some individuals value their privacy enough to pay a mark-up at the firm which collects less information? Or asked in a different way, would it pay for firms to differentiate according to the concern for privacy of consumers? In order to analyse this question, we conducted a number of statistical tests that allowed us to compare the different aforementioned treatments. To obtain results, we compare the average outcome of the treatment and control group in terms of purchases conducted at Firm 1.[56] For example, we can compare the basic control treatment 5 with identical firms (same data requirements and same prices) with the treatment 4 (*different* number of data items and same prices).[57] In the latter treatment, one firm requests more information than the other, meaning that both firms are differentiated. Since participants are randomly assigned to treatments we can be sure to capture a causal effect. If we compare the treatment 4 (same prices and different number of data items) to treatment 3 (*different* prices and different number of data items) we are able to extract the effect of a price difference in terms of shares of purchases at firms that differ on the number of data items they collect. In the following, all numbers are rounded; see Table 3 and 4.

Comparison of treatment 4 and treatment 5: We now compare the situation in which firms are identical (treatment 5) to the situation where they vary on the number of items they

---

[56] *Switchers were encoded in the variables that measured purchases as missing values. We also ran the test with inclusion of switchers in these variables, but the test results do not change much.*
[57] *The privacy policies were always equal at both firms to avoid introducing an additional stimulus.*

Study on monetising privacy

An economic model for pricing personal information

collect (treatment 4). We vary only one stimulus (number of data items collected) from one treatment to the next such that we can be sure of the effect of the stimulus. Moreover, both firms' offers are located right next to each other on the website, such that the difference in data collection is rather obvious to the buyer. We find that the market share of Firm 1, the privacy-friendly firm, is significantly higher in treatment 4 compared to treatment 5.

Table 3 Overview of buyers and their purchases at both firms: all

Treatment	Number of parti-cipants (no. buyers)	No. buyers Zero, one or two tickets bought	Total no. tickets sold	Firm 1 (tickets purchased)		Total no. tickets over two periods (Firm 1)	Firm 1 %-share of all tickets sold (col. 4) rounded	Firm 2 (tickets purchased)		Total no. tickets over two periods (Firm 2)	Firm 2 %-share of all tickets sold (col. 4) rounded
				Period 1	Period 2			Period 1	Period 2		
(1)	(2)	(3)**	(4)**	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
1***	104 (51)	0 - 53 1 - 7 2 - 44	**95**	7	5	12	**13%**	42	41	83	**87%**
2	68 (32)	0 - 36 1 - 9 2 - 23	**55**	20	14	34	**62%**	10	11	21	**38%**
3***	80 (37)	0 - 43 1 - 6 2 - 31	**68**	12	9	21	**31%**	25	22	47	**69%**
4	69 (31)	0 - 38 1 - 4 2 - 27	**58**	26	22	48	**83%**	4	6	10	**17%**
5	122 (41)	0 - 81 1 - 14 2 - 27	**68**	27	15	42	**62%**	13	13	26	**38%**
Total	*443*		*344*	*92*	*65*	*157*	*Avg. 50%*	*94*	*93*	*187*	*Avg. 50%*

*There is no difference between firms in treatment 5; in all other treatments Firm 2 is the privacy-unfriendly firm. **Column (3) adds up to the number of buyers in column (2). The column means that in treatment 1, seven buyers bought one ticket and 44 bought two tickets. Column (4) is based upon these numbers. ***In these treatments, price differences exist.

The difference between the treatment groups is statistically significant based upon the Mann-Whitney tests at the conventional .05-significance level.[58] If there are no price differences and data requirement differences, over 60% of market share in terms of purchases is picked up by Firm 1. This increases to 83% if there are differences in data requirements. If we do the analysis only with loyals, ignoring one-time buyers, the share of tickets sold to loyals of Firm 1 is higher in treatment 4 compared to treatment 5. Thus, if it is very obvious that one firm collects more information than the other, all else being equal, a majority of purchases are made at the privacy-friendly firm.

---

[58] *In more technical terms, the null hypothesis of the Mann-Whitney test is that there is equality in medians. If the test result is not significant, this null cannot be rejected, such that there is not a detectable difference between the groups. We also conducted Chi^2-tests as well as t-tests. These results were significant as well, but are not reported here.*

Study on monetising privacy

An economic model for pricing personal information

This is in line with the literature stating that consumers take privacy protection into account, once it is more salient in the purchase (Tsai et al. 2010; Gideon et al. 2006). In our case, the differences in data collection efforts are obvious in treatment 4. Since consumers had the offers right next to each other, they could compare which information was required from them by the firms.

Comparison of treatment 3 and treatment 4: Next is the comparison of the situation where firms vary on the number of data items they collect (treatment 4) with the situation in which they vary on the data items *and* prices (treatment 3). In the latter case, the privacy-friendly Firm 1 charges €0.50 more compared to its privacy-unfriendly competitor. The share of tickets sold by the privacy-friendly firm now decreases strongly (from 83% to 31%) from treatment 4 to 3. The difference between the treatments is statistically significant based upon the Mann-Whitney tests. This means that the market share of the privacy-friendly firm is significantly reduced, once a competitor charges a lower price, while collecting more information. This result also holds if we only account for loyals. The market share of Firm 1 decreases from 84% to 29% between treatment 4 and 3. However, we also observe a significant share of purchases still conducted at Firm 1, despite the fact that these customers have to pay a higher price. This holds for about a third of buyers.

Table 4 Overview of buyers and their purchases at both firms: loyals

Treatment	Number of participants (no. buyers)	No. buyers who bought **two tickets at the same firm**	Total no. tickets sold to **loyals** col. (6)+(9)	No. of loyal buyers picking Firm 1	No. tickets sold to loyals by Firm 1	**Firm 1 % share of all tickets sold to loyals (6)%(4) rounded**	No. of loyal buyers picking Firm 2	No. tickets sold to loyals by Firm 2	**Firm 2 % share of all tickets sold (10)%(4)**
(1)	(2)	(3)**	(4)	(5)	(6)	(7)	(8)	(9)	(10)
1[***]	104 (51)	43	**86**	4	8	**9%**	39	78	**91%**
2	68 (32)	20	**40**	12	24	**60%**	8	16	**40%**
3[***]	80 (37)	31	**62**	9	18	**29%**	22	44	**71%**
4	69 (31)	25	**50**	21	42	**84%**	4	8	**16%**
5[*]	122 (41)	23	**46**	13	26	**57%**	10	20	**43%**
Total	*443*	*142*	*284*	*59*	*118*	*Avg. 48%*	*83*	*166*	*Avg. 52%*

*There is no difference between firms in treatment 5. Individuals who did not choose Firm 1 either choose Firm 2 or no firm.
**This variable excludes two-time buyers, who switched firms. ***In these treatments, price differences exist.

Comparison of treatment 2 and treatment 5: Again in treatment 5 firms are identical, whereas in treatment 2 they differ on data usage only. We find that there is *not* a significant difference between the two treatment groups. The Mann-Whitney test was not significant and the result is analogous if only loyals are used in the analysis.

Comparison of treatment 1 and treatment 2: Finally, we compare the treatment, where firms only differ on data usage (treatment 2) and on data usage and price (treatment 1). Since we vary only one stimulus (price differences) from one treatment to the next we can be sure of the effect of this variation. Similar and in line with the above observations, the market share of Firm 1 is higher in treatment 2 (62%) than in treatment 1 (13%), considering all one- and two-time sales across both periods. This difference is statistically significant. The share of loyals' purchases at Firm 1 is higher in treatment 2 (60%) compared to treatment 1 (9%).

All in all, we observe the following regularities in the laboratory experiment: in treatments without a price difference (treatments 5, 4, 2), the privacy-friendly firm is able to snatch a higher share of the market, i.e. a higher share of purchases made by participants. In treatments where there is a price difference between firms (treatments 1, 3) the privacy-unfriendly firm obtains a greater market share. The result is similar if we conduct the analysis only for loyals. A higher share of the sales to loyals of the privacy-friendly firms occurs in treatments without price differences. However, once the privacy-unfriendly firm charges a lower price, it can obtain a greater share of all ticket sales to loyals.[59]

6.4   Field and hybrid experiment

The field and hybrid experiment is complementary to the laboratory experiment. For the field and hybrid experiment, we used an experimental website with the same features as in the laboratory. While hybrid participants were invited to the experimental website, visitors in the field did not know that they were part of an experiment.

6.4.1   Place, time period and participants

We conducted the field experiment between September and December 2011. The website featured advertising. Within the time frame we had 2,300 visitors, 87 of which chose a firm ('choosers'), including 10 buyers. One of the reasons for this low number might be the credit card payment facility. Implementing direct debit would have been too risky for this project, but would probably have reduced the number of non-buyers. We will primarily use the number of choosers for the analysis. The hybrid is a mixture of laboratory and field, as the invitations were directed to individuals in different pools at different universities in Germany. We invited the students to the experimental website.

Participation was voluntary. The invitations were sent out in November to TU Berlin students (roughly 900 registered students who had not already participated in the lab); ESMT (about 300 registered students); and Heinrich-Heine University in Düsseldorf (about 1,300 registered

---

[59] *Note that this result holds for a price difference of €0.5 and a ticket price of about €7. We did not make tests with other price differences (or ticket prices) as this would have required a greater number of sessions.*

students). The hybrid experiment ran until the end of December as well. Of 750 individuals who were on the website, 52 chose a firm including 16 bought tickets. In addition, we invited friends to the experimental website. Hybrid participants and friends obtained an extra link, which helped us to identify them in order to separate them from the pure field visitors, which were not personally invited, but found the website on the Internet.

6.4.2   Design of the field and hybrid experiment

The websites used for the hybrid and field experiment were exactly the same as for the laboratory experiment, with the only difference being the graphical design to make it more attractive for visitors. In order to attract buyers to the field website, we had to take a number of advertising measures. For example, after launching the website, we started advertising on the Google, Facebook, VZNetworks, Yahoo and Bing networks and introduced film teasers. One of the outcomes of the field experiment is that it is notoriously difficult to attract potential customers to a new website, because the setting is real and risk aversion of individuals could prevent them from trying out purchases. Because of the low number of buyers, we refrained from sending out questionnaires. However, we have enough observations on choice of a firm in the field, i.e. visitors chose a firm, and typed in their personal information.

6.5   Results from the field and hybrid experiment

For the analysis, we used data from both types of deployments, field and hybrid. This way, it was possible to compare treatments 3 and 4 as well as 4 and 5 (see Table 5). As stated above, the field data are generated in a more natural environment, where we cannot influence external factors that might also influence the individuals' decisions. Therefore, it is important to run experiments in the laboratory as well in order to extract the effects in a more controlled environment. We are particularly interested in whether the share of all choosers (one- and two-time choosers) varies with the treatment as above and whether the same is the case for loyals, i.e. two-time choosers of the same firm. Note that we work with data on choice behaviour; i.e. individuals who chose a firm, entered their data and then either made the purchase or for some reason did not make a purchase.

Comparison of treatment 4 and treatment 5: We compare the situation of two identical firms (treatment 5) with the situation where they differ only on the number of data items they collect (treatment 4), analogous with the laboratory experiment. In this comparison we find that there is no significant difference between the two treatment groups, because the Mann-Whitney test was not significantly different from zero.[60] However, this result is significant at the 0.1 significance level when only using data on loyals, i.e. people who chose the same firm two times, while ignoring one-time choosers. We find that the share of loyal choosers of the privacy-friendly firm is significantly higher in treatment 4 compared to treatment 5 (42%

---

[60] *In more technical terms, the null hypothesis of the Mann-Whitney test is that there is equality in means. If the test result is not significant, this null cannot be rejected, such that there is not a detectable difference between the groups.*

versus 19%). However, in the field treatment 4 the privacy-unfriendly firm has a greater share among loyals.

Table 5 Overview of choosers at Firm 1 and Firm 2 in the field and hybrid experiments

Treatment	No. of participants	All choosers		All loyal choosers	
		Choose Firm 1 (%, rounded)	Did not choose Firm 1 (%, rounded)	Choose Firm 1 (%, rounded)	Did not choose Firm 1 (%, rounded)
3**	67	42	58	5	95
4	29	90	10	42	58
5*	43	16	84	19	81

*There is no difference between firms in treatment 5. Individuals who did not choose Firm 1 either chose Firm 2 or no firm.
** In this treatment, price differences exist.

Comparison of treatment 3 and treatment 4: To extract the effect of a price difference we compare a situation of two firms that collect different amounts of information, but have equal prices (treatment 4) to the situation, where they collect different amounts of information and charge different prices (treatment 3). In treatment 4, the privacy-friendly firm is chosen much more often than not (90%). In treatment 3 the share is 42% for Firm 1. Through the price difference is just €0.50, the share in consumers' choices drops. There is a statistically significant difference in medians between the two treatment groups with respect to the choice of Firm 1 across both periods.[61]

This is similar in the case where we use only observations on the loyals who chose the same firm two times. The share in this market is higher for the privacy-friendly firm in treatment 4 (42%), compared to the situation where the rival charges a lower price (5% only) in treatment 3.

From comparing the treatments 3, 4, 5 in the laboratory and the field for all purchases, we find that the privacy-friendly firm has a much larger market share, if the differences in data collection are obvious and prices are the same. However, once prices change and a privacy-unfriendly competitor charges a lower price the privacy-friendly firm loses market share. But more than a third of purchases by consumers show that they are willing to pay a mark-up at the privacy-friendly firm. In case of loyals a comparison shows inconsistencies, as more two-time buyers pick Firm 2, the unfriendly firm, than Firm 1 in the field treatment 4.

6.6   Assumptions used for the experiments and caveats

The laboratory and the field experiments rely on a number of assumptions. Future research could focus on relaxing these assumptions. In order to reduce the complexity of the theoretical model, we introduced a number of limitations, i.e. we have limited the model to the case of two firms and consumers of two types, with high and low privacy concerns. This is

---

[61] *We applied the Mann-Whitney test just as in the laboratory.*

a simplification, because there are a greater variety of privacy types among consumers. Moreover, in the model consumers are sophisticated, but in the real world they might not anticipate that personalisation could lock them in and lead to higher prices in future periods. But there are also a number of caveats related to the empirical research conducted here.

Research studies based on random sampling of participants generalise to the population from which the sample was drawn. Our research, which follows the common design for economic experiments, is not based on a random sample. We worked for the laboratory with participants registered at the experimental pool of the Technical University of Berlin. While participation in the experiment was based upon a neutral invitation, there is an element of self-selection in terms of motivation to come to the experiment. However, once in the laboratory, participants were randomly assigned to a treatment.

It is debatable whether results obtained on students in a laboratory environment can be generalised to the general population. In general, results from the laboratory are considered to be a useful tool in providing qualitative evidence (Levitt and List 2006). Only to a small extent could we observe more natural behaviour in the field. In fact the field experiment would have needed a much longer running time in order to collect more observations on choice and especially purchase behaviour. One of the questions is whether the experimental manipulation is in fact the *main cause* of the observed choices of participants (internal validity). It relates to other factors that could potentially cause change in choice/behaviour. We have conducted tests on whether the participants in the different treatments were drawn from the same population in terms of age and gender (such that there is no bias due to a selection effect). These tests showed no bias in selection. And we are also planning to conduct tests of ranking and whether participants tend to choose the firm located on the left-hand side. These will be part of a future research study.

7   Conclusions and recommendations

This study is focused on economic transactions; that is, economic exchange intermediated by money, where the disclosure of personal information is a by-product and at times gets the consumer a discount. This excludes transactions which we consider to be social exchange, such as social networks, voluntary participation in anonymous surveys and usage of free services on the Internet. Therefore, the presented research should not be generalised to other populations or transactions that individuals conduct with regards to their personal data.

In order to reduce the complexity of the theoretical model used herein, we introduced a number of assumptions. Future research could focus on relaxing these assumptions. For example, we have limited the model to the case of two firms and consumers of two types, with high and low concern. This is a simplification, because we can assume that there is a greater variety of privacy types among consumers, as in fact we observed during this study. Moreover, in the model consumers are sophisticated, but in the real world they might not anticipate that personalisation could lock them in and lead to higher prices in future periods.

We implemented a simplified version of the model in the laboratory and field. For example, we implemented the version of the model with no transportation costs by placing the offer of the two service providers right next to each other. At the moment, it is too difficult for the consumers to compare different information practices of online service providers. This is exactly the area where we would propose that policy-makers ought to improve transparency for consumers.

Recommendation 1 – If there are little to no differences in the prices offered by service providers on homogeneous goods, a competitor who has a reduced data requirement (privacy-friendly service provider) can obtain a competitive advantage as long as this type of differentiation is obvious to the consumer. The reason is that consumers can – by choosing the service provider with a lower data requirement – reduce their costs of disclosure of personal data.

Recommendation 2 – The regulatory framework should allow for sufficient flexibility that online service providers can offer different menus regarding prices and personal data requirements: from personalised services where identification is required and as such more personal data is collected to less personalised services with fewer requirements for collection of personal data. In fact, it should be required – if no other legal requirements restrict this in specific cases or areas such banking – that service providers also offer services without identification of customers, in order to limit the collection of personal data.

If it is obvious which online service provider collects less personal information a significant share of the market is gained by the privacy-friendly service providers, given that the prices are similar and the products are similar. This observation was especially pronounced in the field experiment.

An increase in transparency of information practices of firms must to be accompanied by an increase in price transparency. Prices should be advertised excluding any discounts for which

42

enisa
European Network
and Information
Security Agency

Study on monetising privacy

An economic model for pricing personal information

consumers are only eligible by providing additional personal data. Moreover, if personal data are used for price discrimination, the consumer should be informed about the fact that this is taking place and what type of discrimination is used.

Recommendation 3 – The differences in data requirements, data protection and privacy policies must be made more visible to consumers in order to enable comparison of terms between online service providers. The more standardised and simple these terms are, the easier comparison will be.

If data practices are difficult to compare, the terms of trade for personal data might not influence the decision of the consumer, who would otherwise pay attention to privacy issues. In this case, the consumer tends to ignore them because of their complexity. The result is that online service provider cannot use privacy settings to fit consumer preferences to obtain a competitive advantage.

Recommendation 4 – Personal profiles are often the base for personalisation of products or services. If portability of profiles among firms is mandated, consumers will face decreased switching costs and benefit from intensified price competition in the market. However the transfer of profiles should be conditioned on the consent of the consumer and in accordance with personal data protection legislation.

The majority of the participants in the study express their concerns for privacy (section 6.3.1). However, the results of the experiments show that when there is a price differentiation the consumers show a tendency to choose cheaper services/goods.

Recommendation 5 – Personal data protection and privacy is a human right. The European Commission, EU Member States and data protection authorities should enforce a clear and consistent legal data protection framework.

8   Glossary

This glossary is complementary to the glossary of terms in ENISA (2011b: 38) and the definitions of key terms in ENISA (2011c: 9). These are only working definitions in the context of this study.

Addressability: The firms' ability to reach consumers based upon their personal data. The degree of addressability can be represented as the proportion of consumers at each point in the market who are in the firm's database; the firm can offer these consumers customised prices. (Source: Chen and Iyer 2002).

Behaviour-based pricing: Behaviour-based pricing is a mechanism whereby a firm uses a consumer's previously observable behaviour to set prices based upon this personal information.

Customisation: Customisation refers to a consumer's own specification of product features to purchase. The customer and not the firm initiate customisation. This is the main difference to personalisation (Source: Arora et al. 2008).

Data protection: Data protection denotes the legal and regulatory codes enacted to protect personal information of individuals.

Lock-in: Lock-in effects arise where consumers are prevented from switching easily and without costs to another provider.

Personalisation: Personalisation refers to a firm's tailored product offerings to an individual consumer based on its data about that consumer. This research follows this terminology and uses the word 'personalisation' for the strategy analysed. The firm and not the consumer initiates personalisation. This is the main difference from customisation (Source: Arora et al. 2008).

Privacy: The term denotes a social convention of keeping specific personal data private, i.e. not releasing it to the public. In the context of this study, the term denotes the asymmetric distribution of personal information between market participants.

Privacy Policy: Privacy policies are terms set by firms, which inform about their personal data handling practices. Consumers who read these terms are informed about the terms of trade for their personal data.

Targeting: A firm's targetability is the ability to predict the preferences and purchase behaviour of consumers for the purpose of customising prices or product offers (Chen, Narasimhan and Zhang 2001).

9   References

Acquisti, A. (2010) 'The Economics of Personal Data and the Economics of Privacy', OECD Roundtable on the Economics of Personal Data and Privacy, December 1.

Acquisti, A. and Varian, H. (2005) 'Conditioning Prices on Purchase History', Marketing Science 24(3): 367–381.

Akçura, T.M. and Srinivasan, K. (2005) 'Customer Intimacy and Cross-Selling Strategy', Management Science 51: 1007–1012.

Akerlof, G.A. (1970) 'The Market for "Lemons": Quality Uncertainty and the Market Mechanism', The Quarterly Journal of Economics 84(3): 488–500.

Arora, N., Drèze, X., Ghose, A., Hess, J.D., Iyengar, R., Jing, B. and Joshi, Y. (2008) 'Putting one-to-one marketing to work: Personalization, customization, and choice', Marketing Letters 19(3-4): 305–321.

Beresford, A.R., Kübler, D.and Preibusch, S. (2010) 'Unwillingness to Pay for Privacy: A Field Experiment', WZB Working Paper.

BITKOM (2010) 12 Millionen Deutsche machen Falschangaben im Web, http://www.bitkom.org/de/presse/66442_62102.aspx

Bohnet, I. and Frey, B.S. (1997) 'Identification in Democratic Society', Journal of Socio-Economics 26(1): 25–38.

Bohnet, I. and Frey, B.S. (1999) 'The Sound of Silence in Prisoner's Dilemma and Dictator Games', Journal of Economic Behavior & Organization 38(1): 43–57.

Calzolari, G. and Pavan, A. (2006) 'On the Optimality of Privacy in Sequential Contracting', Journal of Economic Theory 130(1): 168–204.

Charness, G. and Gneezy, U. (2008) 'What's in a Name? Anonymity and Social Distance in Dictator and Ultimatum Games', Journal of Economic Behavior & Organization 68(1): 29–35.

Chen, Y. and Iyer, G. (2002) 'Research Note: Consumer Addressability and Customized Pricing', Marketing Science 21(2): 197–208.

Chen, Yuxin, Narasimhan, C. and Zhang, Z.J. (2001) 'Individual Marketing and Imperfect Targetability', Marketing Science 20: 23–41.

Conitzer, V., Taylor, C.R. and Wagman, L. (2010) 'Online Privacy and Price Discrimination', Economic Research Initiatives at Duke Working Paper No. 79 (July).

DellaVigna, S. (2009) 'Psychology and Economics: Evidence from the Field', Journal of Economic Literature 47: 315–372.

Dewan, R., Jin, B.and Seidmann, A. (2000) 'Adoption of Internet-Based Product Customization and Pricing Strategy', Journal of Management Information Systems 36(17:2): 9–28.

Dodds, S. (2008) 'Welfare Implications of Confidentiality and Consent in Privacy Regulation', Mimeo, Carleton University.

ENISA (2011a) 'Privacy, Accountability and Trust – Challenges and Opportunities', 2011, http://www.enisa.europa.eu/act/it/library/deliverables/pat-study

ENISA (2011b) 'Survey of accountability, trust, consent, tracking, security and privacy mechanisms in online environments', Jan. 31, 2011, www.enisa.europa.eu/act/it/library/deliverables/survey-pat

ENISA (2011c) 'Managing multiple electronic identities', April 20, 2011, www.enisa.europa.eu/act/it/library/deliverables/mami

Eurobarometer (2011) 'Attitudes on Data Protection and Electronic Identity in the European Union', SPECIAL EUROBAROMETER 359, http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

Fudenberg, D. and Villas-Boas, J.M. (2006) Behavior-based price discrimination and customer recognition, T. Hendershott (ed.) Economics and Information Systems, Vol. 1, Handbooks in Information Systems Series, Amsterdam, Elsevier, pp. 41–47.

Giannetti, C. and Jentzsch, N. (2011) 'Disclosure of Personal Information under the Risk of Privacy Shocks', Mimeo, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1988854

Gideon, J., Cranor, L., Egelman, S. and Acquisti, A. (2006) 'Power Strips, Prophylactics, and Privacy, Oh My!', Institute for Software Research (Paper 24), http://repository.cmu.edu/isr/24

Hermalin, B. and Katz, M. (2006) 'Privacy, Property Rights and Efficiency: The Economics of Privacy as Secrecy', Quantitative Marketing and Economics 4(3): 209–239.

Hoffman, E., McCabe, K. and Smith, V.L. (1996) 'Social Distance and Other-regarding Behavior in Dictator Games', American Economic Review 86(3): 653–660.

Study on monetising privacy

An economic model for pricing personal information

45

Hui, K.-L. and Png, I.P.L. (2006) 'The Economics of Privacy', in Economics and Information Systems, T. Hendershott (ed.), Amsterdam, Elsevier, pp. 471-497.

Huberman, B.A., Adar, E. and Fine, L.R. (2005) 'Valuating Privacy', IEEE Security & Privacy 3(5): 22–25.

Jenni, K.E. and Loewenstein, G. (1997) 'Explaining the "Identifiable Victim Effect"', Journal of Risk and Uncertainty 14(3): 235–257.

Jentzsch, N. (2007) Financial Privacy – An International Comparison of Credit Reporting Systems, Heidelberg, Springer-Verlag.

Kahn, C.M., McAndrews, J. and Roberds, W. (2000) 'A Theory of Transactions Privacy', Working Paper 2000-22, Federal Reserve Bank of Atlanta.

Krahnen, J.P., Rieck, C. and Theissen, E. (1997) Messung individueller Risikoeinstellungen, Center for Financial Studies Working Paper, www.ifk-cfs.de/fileadmin/downloads/publications/wp/97_03.pdf

Lee, D.-J., Ahn J.-H. and Bank, Y. (2011) 'Managing Consumer Privacy Concerns in Personalization: A Strategic Analysis of Privacy Protection', MIS Quarterly 35(2): 423–444.

Levitt, S.D. and List, J.A. (2007) 'What Do Laboratory Experiments Measuring Social Preferences Reveal about the Real World?', Journal of Economic Perspectives 21(2): 153–174.

Pfitzmann, A. and Köhntopp, M. (2000) Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology, avaialble at; http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

Preibusch, S. (2006) 'Personalized Services with Negotiable Privacy Policies', CHI 2006 Workshop on Privacy-Enhanced Personalization, 22 April 2006, Montréal, Canada pp. 29–38.

Smith, H. Jeff, Milberg, Sandra J. and Burke, Sandra J. (1996) 'Information Privacy: Measuring Individuals' Concerns about Organizational Practices', MIS Quarterly 20(June): 167–196.

Stole, L. (2007) 'Price Discrimination and Competition', in M. Armstrong and R. Porter, Handbook of Industrial Organization, Vol. 3, Amsterdam, Elsevier, pp. 2221–2299.

Tsai, J.Y., Egelman, S., Cranor, L. and Acquisti, A. (2010) 'The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study', Information Systems Research, 22(June), 254–268. Available at: http://isr.journal.informs.org/cgi/doi/10.1287/isre.1090.0260.

Villas-Boas, J.M. (1999) 'Dynamic competition with customer recognition', RAND Journal of Economics 30(4): 604–631.

Zhang, J. (2011) 'The Perils of Behavior-Based Personalization', Marketing Science 30(1): 170–186.

46

enisa
European Network
and Information
Security Agency

Study on monetising privacy

An economic model for pricing personal information

10 Annex. Technical appendix

The technical appendix illustrates how the predictions and equilibria described in the report are derived.

One-period model with *r=0*

Consider first the decisions of the consumers. With $r = 0$ each consumer maximises its utility which leads to

$$i^c(\theta_i^c) = \begin{cases} 1 & \text{if } p_A + c(\theta_i^c, d_A) < p_B + c(\theta_i^c, d_B) \\ 1/2 & \text{if } p_A + c(\theta_i^c, d_A) = p_B + c(\theta_i^c, d_B) \\ 0 & \text{if } p_A + c(\theta_i^c, d_A) > p_B + c(\theta_i^c, d_B) \end{cases}$$

Turning to firms' decisions we first analyse different scenarios and then characterize the optimal decisions of firm *A*.

Scenario A $d_A = \underline{d}$: Considering different data requirement decisions of firm B and its potentially optimal pricing decisions leads to the following profits for B and A :

In order to earn positive profits, firm A has to ensure that B reacts as described in the third line. Thus firm *A* will try to set p_A such that

$$\Pi_B^3 \ge \max\{\Pi_B^1, \Pi_B^2\}$$

Taking into account different parameter constellations, the above inequality leads to

$$p_A = \begin{cases} 0 & \text{if} \quad q \ge \Delta c(\overline{\theta}) \text{ and } \Delta c(\overline{\theta}) \ge (1-\mu)\Delta c(\underline{\theta}) + \mu q \\ \frac{1}{\mu}(\Delta c(\overline{\theta}) - (1-\mu)\Delta c(\underline{\theta}) - \mu q) & \text{if} \quad q \ge \Delta c(\overline{\theta}) \text{ and } \Delta c(\overline{\theta}) \le (1-\mu)\Delta c(\underline{\theta}) + \mu q \\ \frac{1-\mu}{\mu}(q - \Delta c(\underline{\theta})) & \text{if} \quad \Delta c(\overline{\theta}) \ge q \ge \Delta c(\underline{\theta}) \\ 0 & \text{if} \quad \Delta c(\underline{\theta}) \ge q \end{cases}$$

Scenario B $d_A = \overline{d}$: Proceeding as above we obtain:

$$\begin{aligned} d_B = \overline{d} &\rightarrow \Pi_B^1 := p_A + q & \Pi_A^1 = 0 \\ d_B = \underline{d} &\rightarrow \Pi_B^2 := p_A + \Delta c(\underline{\theta}) & \Pi_A^2 = 0 \\ d_B = \underline{d} &\rightarrow \Pi_B^3 := (p_A + \Delta c(\overline{\theta}))\mu & \Pi_A^3 = (p_A + q)(1-\mu) \end{aligned}$$

Analyzing
$$\Pi_B^3 \ge \max\{\Pi_B^1, \Pi_B^2\}$$

leads to the following pricing decisions of firm A

$$p_A = \begin{cases} -q & \text{if} \quad q \ge \Delta c(\overline{\theta}) \\ \frac{1}{1-\mu}\left[\mu\Delta c(\overline{\theta}) - q\right] & \text{if} \quad \Delta c(\overline{\theta}) \ge q \ge \Delta c(\underline{\theta}) \\ \frac{1}{1-\mu}\left[\mu\Delta c(\overline{\theta}) - \Delta c(\underline{\theta})\right] & \text{if} \quad \Delta c(\underline{\theta}) \ge q \text{ and } \Delta c(\overline{\theta}) \ge \frac{1}{\mu}\left[\Delta c(\underline{\theta}) - (1-\mu)q\right] \\ -q & \text{if} \quad \Delta c(\underline{\theta}) \ge q \text{ and } \Delta c(\overline{\theta}) \le \frac{1}{\mu}\left[\Delta c(\underline{\theta}) - (1-\mu)q\right] \end{cases}$$

Substituting these prices in firm A's profit function and comparing its profits, we get the following equilibrium data requirement decisions and equilibrium profits

$q \geq \Delta c(\bar{\theta})$

$d_A = \bar{d} \to d_B = \bar{d} \quad \Pi_A = 0 \quad \text{if} \quad q \geq \frac{1}{\mu}(\Delta c(\bar{\theta}) - (1-\mu)\Delta c(\underline{\theta}))$

$d_A = \underline{d} \to d_B = \bar{d} \quad \Pi_A = \Delta c(\bar{\theta}) - (1-\mu)\Delta c(\underline{\theta}) - \mu q \quad \text{if} \quad q \leq \frac{1}{\mu}(\Delta c(\bar{\theta}) - (1-\mu)\Delta c(\underline{\theta}))$

$q \in \left[\Delta c(\bar{\theta}), \Delta c(\underline{\theta})\right]$

$d_A = \underline{d} \to d_B = \bar{d} \quad \Pi_A = (1-\mu)(q - \Delta c(\underline{\theta})) \quad \text{if} \quad q \geq (1-\mu)\Delta c(\underline{\theta}) + \mu\Delta c(\bar{\theta})$

$d_A = \bar{d} \to d_B = \underline{d} \quad \Pi_A = \mu(\Delta c(\bar{\theta}) - q) \quad \text{if} \quad q \leq (1-\mu)\Delta c(\underline{\theta}) + \mu\Delta c(\bar{\theta})$

$q \leq \Delta c(\underline{\theta})$

$d_A = \bar{d} \to d_B = \underline{d} \quad \Pi_A = \mu\Delta c(\bar{\theta}) - \Delta c(\underline{\theta}) + (1-\mu)q \quad \text{if} \quad q \geq \frac{1}{1-\mu}\left[\mu\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right]$

$d_A = \underline{d} \to d_B = \underline{d} \quad \Pi_A = 0 \quad \text{if} \quad q \leq \frac{1}{1-\mu}\left[\mu\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right]$

One-period model with $r > 0$

Solving by backward induction we first turn to the consumers and compute the location of the indifferent consumers, given any combination of prices and data requirements.

$$i^c(\theta_{i^c}) = \begin{cases} \frac{1}{2} - \frac{p_A - p_B + c(\theta_{i^c}, d_A) - c(\theta_{i^c}, d_B)}{2r} & \text{if } i^c(\theta_{i^c}) \in [0,1] \\ 1 \text{ if } i^c(\theta_{i^c}) > 1 \\ 0 \text{ otherwise} \end{cases}$$

This leads to the following market shares for firm A and B:

$$n_A = \mu i^c(\bar{\theta}) + (1-\mu)i^c(\underline{\theta})$$

$$n_B = 1 - n_A$$

Then, solving for firm B's price reaction function yields:

$$p_B^* = \frac{1}{2}(r + p_A + \mu(c(\bar{\theta}, d_A) - c(\bar{\theta}, d_B)) + (1-\mu)(c(\underline{\theta}, d_A) - c(\underline{\theta}, d_B)) - q\alpha_B)$$

Now, comparing profits under the two different data requirements leads to the following:

$$\Pi_B = \begin{cases} \Pi_B^1 := \frac{1}{8r}(r + p_A + \mu(c(\bar{\theta}, d_A) - c(\bar{\theta}, \underline{d})) + (1-\mu)(c(\underline{\theta}, d_A) - c(\underline{\theta}, \underline{d})))^2 & d_B = \underline{d} \\ \Pi_B^2 := \frac{1}{8r}(r + p_A + \mu(c(\bar{\theta}, d_A) - c(\bar{\theta}, \bar{d})) + (1-\mu)(c(\underline{\theta}, d_A) - c(\underline{\theta}, \bar{d})) + q)^2 & d_B = \bar{d} \end{cases}$$

Thus, firm B's data requirement decision will be:

$$d_B^* = \begin{cases} \underline{d} \text{ if } \mu\Delta c(\bar{\theta}) + (1-\mu)\Delta c(\underline{\theta}) > q \\ \bar{d} \text{ otherwise} \end{cases}$$

Then regarding firm A, we can compute the pricing function:

$$p_A^* = \frac{1}{2}(3r - \mu(c(\bar{\theta}, d_A) - c(\bar{\theta}, d_B)) - (1-\mu)(c(\underline{\theta}, d_A) - c(\underline{\theta}, d_B)) - q\alpha_A - q\alpha_B)$$

This leads to the following profits:

Study on monetising privacy

An economic model for pricing personal information

$$\Pi_A = \frac{1}{16r}(3r - \mu(c(\overline{\theta},d_A) - c(\overline{\theta},d_B)) - (1-\mu)(c(\underline{\theta},d_A) - c(\underline{\theta},d_B)) + q\alpha_A - q\alpha_B)^2$$

We now have to consider two different cases separately:

1. Case: $\mu\Delta c(\overline{\theta}) + (1-\mu)\Delta c(\underline{\theta}) > q$

Taking into account firm *B*'s decisions, we get the following price for *A*:

$$p_A^* = \frac{1}{2}(3r - \mu(c(\overline{\theta},d_A) - c(\overline{\theta},\underline{d})) - (1-\mu)(c(\underline{\theta},d_A) - c(\underline{\theta},\underline{d})) - q\alpha_A)$$

This in turn leads to the comparison of the following profits:

$$\Pi_A = \begin{cases} \Pi_A^1 := \frac{9r}{16} & d_A = \underline{d} \\ \Pi_A^2 := \frac{1}{16r}(3r - \mu(c(\overline{\theta},\overline{d}) - c(\overline{\theta},\underline{d})) - (1-\mu)(c(\underline{\theta},\overline{d}) - c(\underline{\theta},\underline{d})) + q)^2 & d_A = \overline{d} \end{cases}$$

As in this case $\mu\Delta c(\overline{\theta}) + (1-\mu)\Delta c(\underline{\theta}) > q$, we get as the optimal data requirement decision:

$$d_A^* = \underline{d}$$

Collecting the decisions, the equilibrium in this case is:

$$(d_A^* = \underline{d}, p_A^* = \frac{3r}{2}), (d_B^* = \underline{d}, p_B^* = \frac{5r}{4})$$

2. Case: $\mu\Delta c(\overline{\theta}) + (1-\mu)\Delta c(\underline{\theta}) < q$

In this case the pricing function is:

$$p_A^* = \frac{1}{2}(3r - \mu(c(\overline{\theta},d_A) - c(\overline{\theta},\overline{d})) - (1-\mu)(c(\underline{\theta},d_A) - c(\underline{\theta},\overline{d})) - q\alpha_A - q)$$

Thus, the profits, which have to be compared, are now:

$$\Pi_A = \begin{cases} \Pi_A^1 := \frac{1}{16r}(3r + \mu(c(\overline{\theta},\overline{d}) - c(\overline{\theta},\underline{d})) + (1-\mu)(c(\underline{\theta},\overline{d}) - c(\underline{\theta},\underline{d})) - q)^2 & d_A = \underline{d} \\ \Pi_A^2 := \frac{9r}{16} & d_A = \overline{d} \end{cases}$$

As in this case it holds that $\mu\Delta c(\overline{\theta}) + (1-\mu)\Delta c(\underline{\theta}) < q$, we can state:

$$d_A^* = \overline{d}$$

This gives the following equilibrium:

$$(d_A^* = \overline{d}, p_A^* = \frac{3r - 2q}{2}), (d_B^* = \overline{d}, p_B^* = \frac{5r - 4q}{4})$$

In both equilibria market shares are equal to:

$$n_A^* = \frac{3}{8}, n_B^* = \frac{5}{8}$$

Two-period model with *r=0*

Scenario a): $0 > \Delta b(\underline{\theta}) > \Delta b(\overline{\theta})$

To characterise the equilibria in the two-period model we start with the second period where we analyse the firms' pricing decisions for $d_A = \overline{d} > \underline{d} = d_B$ and $d_A = \underline{d} < \overline{d} = d_B$. We then turn to the first period where we analyse both the firms' pricing decisions as well as the firms' profits for different data requirement decisions of firm B. Using these results and comparing

Study on monetising privacy

An economic model for pricing personal information

enisa
European Network
and Information
Security Agency

49

the profits of firm A with $d_A = \bar{d}$ and $d_A = \underline{d}$ allows us to determine the equilibrium in the overall game. Note further that $d_A = d_B$ leads to zero profits in both periods.

Second period prices and profits

a) $d_A = \bar{d} > d_B = \underline{d}$: Using the potentially optimal pricing decisions of firm B, firm B's and A's second period profits are given by

$$\Pi^1_{B,2} := p_{A,2} + \Delta c(\underline{\theta}) \quad ; \quad \Pi^1_{A,2} = 0$$
$$\Pi^2_{B,2} := (p_{A,2} + \Delta c(\bar{\theta}))\mu \quad ; \quad \Pi^2_{A,2} = (p_{A,2} + q)(1 - \mu)$$
$$\Pi^3_{B,2} := 0 \quad ; \quad \Pi^3_{A,2} = (q - \Delta c(\bar{\theta}))$$

As in the one-period model, firm A tries to induce firm B to set its prices such that firm A earns the highest possible profit. Comparing profits and calculating firm B's best response as well as the implied profit of firm A, we get the following pricing decisions of firm A:

$$p_{A,2} = \begin{cases} -\Delta c(\bar{\theta}) & \text{if} \quad q \geq \Delta c(\bar{\theta}) + \frac{1}{\mu}\left[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right] \\ \frac{1}{1-\mu}\left[\mu\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right] & \text{if} \quad q \leq \Delta c(\bar{\theta}) + \frac{1}{\mu}\left[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right] \\ -q & \text{if} \quad q \leq \frac{1}{1-\mu}\left[\Delta c(\underline{\theta}) - \mu\Delta c(\bar{\theta})\right] \end{cases}$$

Using these prices the firms' second period profits are given by

$$\Pi_{A,2} = \begin{cases} q - \Delta c(\bar{\theta}) & \text{if} \quad q \geq \Delta c(\bar{\theta}) + \frac{1}{\mu}\left[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right] \\ \mu\Delta c(\bar{\theta}) - \Delta c(\underline{\theta}) + (1-\mu)q & \text{if} \quad q \leq \Delta c(\bar{\theta}) + \frac{1}{\mu}\left[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right] \\ 0 & \text{if} \quad q \leq \frac{1}{1-\mu}\left[\Delta c(\underline{\theta}) - \mu\Delta c(\bar{\theta})\right] \end{cases}$$

$$\Pi_{B,2} = \begin{cases} 0 & \text{if} \quad q \geq \Delta c(\bar{\theta}) + \frac{1}{\mu}\left[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right] \\ \frac{\mu}{1-\mu}\left[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right] & \text{if} \quad q \leq \Delta c(\bar{\theta}) + \frac{1}{\mu}\left[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right] \\ \Delta c(\underline{\theta}) - q & \text{if} \quad q \leq \frac{1}{1-\mu}\left[\Delta c(\underline{\theta}) - \mu\Delta c(\bar{\theta})\right] \end{cases}$$

b) $d_A = \underline{d} < d_B = \bar{d}$: Employing the potentially optimal pricing decisions of firm B, firm B's and A's second period profits are given by

$$\Pi^1_{B,2} := p_A + q - \Delta c(\bar{\theta}) \quad ; \quad \Pi^1_{A,2} = 0$$
$$\Pi^2_{B,2} := (p_A + q - \Delta c(\underline{\theta}))(1 - \mu) \quad ; \quad \Pi^2_{A,2} = p_A\mu$$
$$\Pi^3_{B,2} := 0 \quad ; \quad \Pi^3_{A,2} = \Delta c(\underline{\theta}) - q$$

Proceeding as above and calculating the firm B's best response and the implied profit of firm A, we get the following pricing decisions of firm A:

$$p_{A,2} = \begin{cases} 0 & \text{if} \quad q \geq \frac{1}{\mu}\left[\Delta c(\bar{\theta}) - (1-\mu)\Delta c(\underline{\theta})\right] \\ \frac{1}{\mu}\left[\Delta c(\bar{\theta}) - (1-\mu)\Delta c(\underline{\theta})\right] - q & \text{if} \quad q \leq \frac{1}{\mu}\left[\Delta c(\bar{\theta}) - (1-\mu)\Delta c(\underline{\theta})\right] \\ \Delta c(\underline{\theta}) - q & \text{if} \quad q \leq \frac{1}{1-\mu}\left[(2-\mu)\Delta c(\underline{\theta}) - \Delta c(\bar{\theta})\right] \end{cases}$$

The firms' second period profits can be written as

Study on monetising privacy

An economic model for pricing personal information

$$\Pi_{A,2} = \begin{cases} 0 & \text{if} \quad q \geq \frac{1}{\mu}\left[\Delta c(\bar{\theta}) - (1-\mu)\Delta c(\underline{\theta})\right] \\ \Delta c(\bar{\theta}) - (1-\mu)\Delta c(\underline{\theta}) - \mu q & \text{if} \quad q \leq \frac{1}{\mu}\left[\Delta c(\bar{\theta}) - (1-\mu)\Delta c(\underline{\theta})\right] \\ \Delta c(\underline{\theta}) - q & \text{if} \quad q \leq \frac{1}{1-\mu}\left[(2-\mu)\Delta c(\underline{\theta}) - \Delta c(\bar{\theta})\right] \end{cases}$$

$$\Pi_{B,2} = \begin{cases} q - \Delta c(\bar{\theta}) & \text{if} \quad q \geq \frac{1}{\mu}\left[\Delta c(\bar{\theta}) - (1-\mu)\Delta c(\underline{\theta})\right] \\ \frac{1-\mu}{\mu}\left[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right] & \text{if} \quad q \leq \frac{1}{\mu}\left[\Delta c(\bar{\theta}) - (1-\mu)\Delta c(\underline{\theta})\right] \\ 0 & \text{if} \quad q \leq \frac{1}{1-\mu}\left[(2-\mu)\Delta c(\underline{\theta}) - \Delta c(\bar{\theta})\right] \end{cases}$$

First period prices and firm B 's data requirement decision

In order to calculate the firms' pricing decisions in the first period as well as firm B's profit given either $d_B = \bar{d}$ or $d_B = \underline{d}$ we have to consider the second period profits given above.

a) $d_A = \bar{d}$: In this case there are 4 different parameter constellations to be analysed.

Case 1): $q \geq \Delta c(\bar{\theta}) + \frac{1}{\mu}\left[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right]$; Employing firm B's potentially optimal pricing decisions in the first period as well as the second period profits given above we get the following overall profits for firm B and A :

$$\begin{array}{llll}
d_B = \bar{d} & \rightarrow & \Pi_B^1 := p_{A,1} + q & ; \quad \Pi_A^1 = 0 \\
d_B = \underline{d} & \rightarrow & \Pi_B^2 := p_{A,1} + \Delta c(\underline{\theta}) & ; \quad \Pi_A^2 = q - \Delta c(\bar{\theta}) \\
d_B = \underline{d} & \rightarrow & \Pi_B^3 := \mu(p_{A,1} + \Delta c(\bar{\theta})) & ; \quad \Pi_A^3 = (p_{A,1} + q)(1-\mu) + q - \Delta c(\bar{\theta}) \\
d_B = \underline{d} & \rightarrow & \Pi_B^4 := 0 & ; \quad \Pi_A^4 = q - \Delta c(\bar{\theta}) + q - \Delta c(\bar{\theta})
\end{array}$$

Using $\Pi_B^1 \geq \Pi_B^2$ and comparing profits shows that firm A is not able to induce firm B to choose $\underline{d}$. Hence, we get $d_B = \bar{d}$ and

$$\Pi_A = \Pi_B = 0$$

Case 2): $\Delta c(\bar{\theta}) + \frac{1}{\mu}\left[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right] \geq q \geq \Delta c(\underline{\theta}) + \frac{\mu}{1-\mu}\left[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right]$; Here overall profits for firm B and A are given by

$$\begin{array}{llll}
d_B = \bar{d} & \rightarrow & \Pi_B^1 := p_{A,1} + q & ; \quad \Pi_A^1 = 0 \\
d_B = \underline{d} & \rightarrow & \Pi_B^2 := p_{A,1} + \Delta c(\underline{\theta}) + \frac{\mu}{1-\mu}\left[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right] & ; \quad \Pi_A^2 = \mu\Delta c(\bar{\theta}) - \Delta c(\underline{\theta}) + (1-\mu)q \\
d_B = \underline{d} & \rightarrow & \Pi_B^3 := \mu(p_{A,1} + \Delta c(\bar{\theta})) + \frac{\mu}{1-\mu}\left[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right] & ; \quad \Pi_A^3 = (p_{A,1} + q)(1-\mu) + \mu\Delta c(\bar{\theta}) - \Delta c(\underline{\theta}) + (1-\mu)q
\end{array}$$

Again, employing $\Pi_B^1 \geq \Pi_B^2$ and comparing profits shows firm A can ensure itself strictly positive profits by inducing firm B to choose $d_B = \underline{d}$ only if $\mu \leq 0.5$. In this case the firms' profits are given by

$$\Pi_A = \frac{1}{1-\mu}\left[q + \mu(3-2\mu)(\Delta c(\bar{\theta}) - q) - \Delta c(\underline{\theta})\right]$$

$$\Pi_B = \frac{\mu}{(1-\mu)^2}\left[\Delta c(\bar{\theta})(2-\mu) - \Delta c(\underline{\theta}) - (1-\mu)q\right]$$

Study on monetising privacy

An economic model for pricing personal information

Case 3): $\Delta c(\underline{\theta}) + \frac{\mu}{1-\mu}\left[\Delta c(\overline{\theta}) - \Delta c(\underline{\theta})\right] \geq q \geq \frac{1}{1-\mu}\left[\Delta c(\underline{\theta}) - \mu\Delta c(\overline{\theta})\right]$; Proceeding as above we have

$$d_B = \overline{d} \quad \rightarrow \quad \Pi_B^1 := p_{A,1} + q \qquad\qquad\qquad\qquad ; \quad \Pi_A^1 = 0$$

$$d_B = \underline{d} \quad \rightarrow \quad \Pi_B^2 := p_{A,1} + \Delta c(\underline{\theta}) + \frac{\mu}{1-\mu}\left[\Delta c(\overline{\theta}) - \Delta c(\underline{\theta})\right] \quad ; \quad \Pi_A^2 = \mu\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) + (1-\mu)q$$

$$d_B = \underline{d} \quad \rightarrow \quad \Pi_B^3 := \mu(p_{A,1} + \Delta c(\overline{\theta})) + \frac{\mu}{1-\mu}\left[\Delta c(\overline{\theta}) - \Delta c(\underline{\theta})\right] \quad ; \quad \Pi_A^3 = (p_{A,1} + q)(1-\mu) + \mu\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) + (1-\mu)q$$

Using $\Pi_B^2 \geq \Pi_B^1$, firm A sets its first period price such that $\Pi_B^2 = \Pi_B^3$ which leads to

$$\Pi_A = 2\left[\mu\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) + (1-\mu)q\right]$$

$$\Pi_B = 2\frac{\mu}{1-\mu}\left[\Delta c(\overline{\theta}) - \Delta c(\underline{\theta})\right]$$

Case 4): $\frac{1}{1-\mu}\left[\Delta c(\underline{\theta}) - \mu\Delta c(\overline{\theta})\right] \geq q$; The profits of firm B and A are given by

$$d_B = \overline{d} \quad \rightarrow \quad \Pi_B^1 := p_{A,1} + q \qquad\qquad\qquad ; \quad \Pi_A = 0$$

$$d_B = \underline{d} \quad \rightarrow \quad \Pi_B^2 := p_{A,1} + \Delta c(\underline{\theta}) + \Delta c(\underline{\theta}) - q \qquad ; \quad \Pi_A = 0$$

$$d_B = \underline{d} \quad \rightarrow \quad \Pi_B^3 := \mu(p_{A,1} + \Delta c(\overline{\theta})) + \Delta c(\underline{\theta}) - q \quad ; \quad \Pi_A = (p_{A,1} + q)(1-\mu)$$

Since again $\Pi_B^2 \geq \Pi_B^1$ and q is small enough, firm A chooses $p_A = -q$ which leads to

$$\Pi_A = 0 \text{ and } \Pi_B = 2\left[\Delta c(\underline{\theta}) - q\right]$$

b) $d_A = \underline{d}$: Again there are 4 different parameter constellations to be analysed.

Case 1): $q \geq \frac{1}{\mu}\left[\Delta c(\overline{\theta}) - (1-\mu)\Delta c(\underline{\theta})\right]$; The firms' reduced profits are given by

$$d_B = \underline{d} \quad \rightarrow \quad \Pi_B^1 := p_{A,1} \qquad\qquad\qquad\qquad ; \quad \Pi_A = 0$$

$$d_B = \overline{d} \quad \rightarrow \quad \Pi_B^2 := p_{A,1} + q - \Delta c(\overline{\theta}) + q - \Delta c(\overline{\theta}) \qquad ; \quad \Pi_A = 0$$

$$d_B = \overline{d} \quad \rightarrow \quad \Pi_B^3 := (p_{A,1} + q - \Delta c(\underline{\theta}))(1-\mu) + q - \Delta c(\overline{\theta}) \quad ; \quad \Pi_A = p_{A,1}\mu$$

Proceeding as above we obtain

$$p_A = 0 \rightarrow \Pi_A = 0 \text{ and } \Pi_B = 0$$

Case 2):
$\frac{1}{\mu}\left[\Delta c(\overline{\theta}) - (1-\mu)\Delta c(\underline{\theta})\right] \geq q \geq \max\left\{\Delta c(\overline{\theta}) - \frac{1-\mu}{\mu}\left[\Delta c(\overline{\theta}) - \Delta c(\underline{\theta})\right], \frac{1}{1-\mu}\left[(2-\mu)\Delta c(\underline{\theta}) - \Delta c(\overline{\theta})\right]\right\}$;

In this case the firms' profits are given by

$$d_B = \underline{d} \quad \rightarrow \quad \Pi_B^1 := p_{A,1} \qquad\qquad\qquad\qquad ; \quad \Pi_A = 0$$

$$d_B = \overline{d} \quad \rightarrow \quad \Pi_B^2 := p_{A,1} + q - \Delta c(\overline{\theta}) + \frac{1-\mu}{\mu}\left[\Delta c(\overline{\theta}) - \Delta c(\underline{\theta})\right] \qquad ; \quad \Pi_A = \Delta c(\overline{\theta}) - (1-\mu)\Delta c(\underline{\theta}) - \mu q$$

$$d_B = \overline{d} \quad \rightarrow \quad \Pi_B^3 := (p_{A,1} + q - \Delta c(\underline{\theta}))(1-\mu) + \frac{1-\mu}{\mu}\left[\Delta c(\overline{\theta}) - \Delta c(\underline{\theta})\right] \quad ; \quad \Pi_A = p_{A,1}\mu + \Delta c(\overline{\theta}) - (1-\mu)\Delta c(\underline{\theta}) - \mu q$$

Using $\Pi_B^2 \geq \Pi_B^1$ firm A sets $p_{A,1}$ such that $\Pi_B^2 = \Pi_B^3$ which leads to

An economic model for pricing personal information

$$\Pi_A = 2\left[\Delta c(\bar{\theta}) - (1-\mu)\Delta c(\underline{\theta}) - \mu q\right]$$

$$\Pi_B = 2\frac{1-\mu}{\mu}\left[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right]$$

Case 3): $\Delta c(\bar{\theta}) - \frac{1-\mu}{\mu}\left[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right] \geq q \geq \frac{1}{1-\mu}\left[(2-\mu)\Delta c(\underline{\theta}) - \Delta c(\bar{\theta})\right]$; Calculating the firms' profits we get

$$
\begin{array}{llll}
d_B = \underline{d} & \rightarrow & \Pi_B^1 := p_{A,1} & ; \quad \Pi_A = 0 \\
d_B = \bar{d} & \rightarrow & \Pi_B^2 := p_{A,1} + q - \Delta c(\bar{\theta}) + \frac{1-\mu}{\mu}\left[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right] & ; \quad \Pi_A = \Delta c(\bar{\theta}) - (1-\mu)\Delta c(\underline{\theta}) - \mu q \\
d_B = \bar{d} & \rightarrow & \Pi_B^3 := (p_{A,1} + q - \Delta c(\underline{\theta}))(1-\mu) + \frac{1-\mu}{\mu}\left[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right] & ; \quad \Pi_A = p_{A,1}\mu + \Delta c(\bar{\theta}) - (1-\mu)\Delta c(\underline{\theta}) - \mu q
\end{array}
$$

and thus $\Pi_B^1 \geq \Pi_B^2$. Using $\Pi_B^3 = \Pi_B^1$ leads to

$$\Pi_A = \Delta c(\bar{\theta}) - 2(1-\mu)\Delta c(\underline{\theta}) + q(1-2\mu)$$

$$\Pi_B = \frac{1-\mu}{\mu}\left[\Delta c(\bar{\theta}) + q - 2\Delta c(\underline{\theta})\right]$$

Case 4): $q \leq \frac{1}{1-\mu}\left[(2-\mu)\Delta c(\underline{\theta}) - \Delta c(\bar{\theta})\right]$; Analyzing

$$
\begin{array}{llll}
d_B = \underline{d} & \rightarrow & \Pi_B^1 := p_{A,1} & ; \quad \Pi_A = 0 \\
d_B = \bar{d} & \rightarrow & \Pi_B^2 := p_{A,1} + q - \Delta c(\bar{\theta}) & ; \quad \Pi_A = \Delta c(\underline{\theta}) - q \\
d_B = \bar{d} & \rightarrow & \Pi_B^3 := (p_{A,1} + q - \Delta c(\underline{\theta}))(1-\mu) & ; \quad \Pi_A = p_{A,1}\mu + \Delta c(\underline{\theta}) - q
\end{array}
$$

reveals $\Pi_B^1 \geq \Pi_B^2$. Comparing Π_B^1 and Π_B^3 shows that firm A is not able to induce firm B to choose $\bar{d}$. Hence, we get $d_B = \underline{d}$ and

$$\Pi_A = \Pi_B = 0$$

Collecting these results and comparing the profits of firm A for $d_A = \bar{d}$ and $d_A = \underline{d}$ we can deduce the profit maximising data requirement decision of firm A and thus the overall equilibrium of the game. However, we first have to compare the critical values of q which leads to

$$1)\, \Delta c(\bar{\theta}) + \frac{1}{\mu}\left[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right] > \frac{1}{\mu}\left[\Delta c(\bar{\theta}) - (1-\mu)\Delta c(\underline{\theta})\right]$$

$$2)\, \frac{1}{\mu}\left[\Delta c(\bar{\theta}) - (1-\mu)\Delta c(\underline{\theta})\right] \geq \Delta c(\underline{\theta}) + \frac{\mu}{1-\mu}\left[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right] \Leftrightarrow \mu \leq 0.6$$

$$3)\, \Delta c(\underline{\theta}) + \frac{\mu}{1-\mu}\left[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right] > \Delta c(\bar{\theta}) - \frac{1-\mu}{\mu}\left[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\right]$$

Study on monetising privacy

An economic model for pricing personal information

$$4)\, \Delta c(\bar{\theta}) - \frac{1-\mu}{\mu}\Big[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\Big] ?\, \frac{1}{1-\mu}\Big[\Delta c(\underline{\theta}) - \mu\Delta c(\bar{\theta})\Big] \Leftrightarrow \mu\,?\,0.4$$

$$5)\, \Delta c(\bar{\theta}) - \frac{1-\mu}{\mu}\Big[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\Big] ?\, \frac{1}{1-\mu}\Big[(2-\mu)\Delta c(\underline{\theta}) - \Delta c(\bar{\theta})\Big] \Leftrightarrow \mu\,?\,0.2$$

$$6)\, \frac{1}{1-\mu}\Big[\Delta c(\underline{\theta}) - \mu\Delta c(\bar{\theta})\Big] > \frac{1}{1-\mu}\Big[(2-\mu)\Delta c(\underline{\theta}) - \Delta c(\bar{\theta})\Big]$$

Assuming $\mu \in [0.4, 0.6]$ we get the following outcomes:

$$1.)\, q \geq \Delta c(\bar{\theta}) + \frac{1}{\mu}\Big[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\Big]$$

$$\rightarrow d_A = \bar{d} \rightarrow d_B = \bar{d} \rightarrow \Pi_A = 0$$

$$2.)\, \Delta c(\bar{\theta}) + \frac{1}{\mu}\Big[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\Big] \geq q \geq \frac{1}{\mu}\Big[\Delta c(\bar{\theta}) - (1-\mu)\Delta c(\underline{\theta})\Big]$$

$$\rightarrow d_A = \bar{d} \rightarrow d_B = \underline{d} \rightarrow \Pi_A = \frac{1}{1-\mu}\Big[q + \mu(3-2\mu)(\Delta c(\bar{\theta}) - q) - \Delta c(\underline{\theta})\Big]$$

$$3.)\, \frac{1}{\mu}\Big[\Delta c(\bar{\theta}) - (1-\mu)\Delta c(\underline{\theta})\Big] \geq q \geq \Delta c(\underline{\theta}) + \frac{\mu}{1-\mu}\Big[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\Big]$$

$$\rightarrow d_A = \bar{d} \rightarrow d_B = \underline{d} \rightarrow \Pi_A = \frac{1}{1-\mu}\Big[q + \mu(3-2\mu)(\Delta c(\bar{\theta}) - q) - \Delta c(\underline{\theta})\Big]$$

$$\rightarrow d_A = \underline{d} \rightarrow d_B = \bar{d} \rightarrow \Pi_A = 2\Big[\Delta c(\bar{\theta}) - (1-\mu)\Delta c(\underline{\theta}) - \mu q\Big]$$

$$4.)\, \Delta c(\underline{\theta}) + \frac{\mu}{1-\mu}\Big[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\Big] \geq q \geq \Delta c(\bar{\theta}) - \frac{1-\mu}{\mu}\Big[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\Big]$$

$$\rightarrow d_A = \bar{d} \rightarrow d_B = \underline{d} \rightarrow \Pi_A = 2\Big[\mu\Delta c(\bar{\theta}) - \Delta c(\underline{\theta}) + (1-\mu)q\Big]$$

$$\rightarrow d_A = \underline{d} \rightarrow d_B = \bar{d} \rightarrow \Pi_A = 2\Big[\Delta c(\bar{\theta}) - (1-\mu)\Delta c(\underline{\theta}) - \mu q\Big]$$

$$5.)\, \Delta c(\bar{\theta}) - \frac{1-\mu}{\mu}\Big[\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})\Big] \geq q \geq \frac{1}{1-\mu}\Big[\Delta c(\underline{\theta}) - \mu\Delta c(\bar{\theta})\Big]$$

$$\rightarrow d_A = \bar{d} \rightarrow d_B = \underline{d} \rightarrow \Pi_A = 2\Big[\mu\Delta c(\bar{\theta}) - \Delta c(\underline{\theta}) + (1-\mu)q\Big]$$

$$\rightarrow d_A = \underline{d} \rightarrow d_B = \bar{d} \rightarrow \Pi_A = \Delta c(\bar{\theta}) - 2(1-\mu)\Delta c(\underline{\theta}) + q(1-2\mu)$$

$$6.)\, \frac{1}{1-\mu}\Big[\Delta c(\underline{\theta}) - \mu\Delta c(\bar{\theta})\Big] \geq q \geq \frac{1}{1-\mu}\Big[(2-\mu)\Delta c(\underline{\theta}) - \Delta c(\bar{\theta})\Big]$$

$$\rightarrow d_A = \bar{d} \rightarrow d_B = \underline{d} \rightarrow \Pi_A = 0$$

$$\rightarrow d_A = \underline{d} \rightarrow d_B = \bar{d} \rightarrow \Pi_A = \Delta c(\bar{\theta}) - 2(1-\mu)\Delta c(\underline{\theta}) + q(1-2\mu)$$

$$7.)\, \frac{1}{1-\mu}\Big[(2-\mu)\Delta c(\underline{\theta}) - \Delta c(\bar{\theta})\Big] \geq q$$

$$\rightarrow d_A = \underline{d} \rightarrow d_B = \underline{d} \rightarrow \Pi_A = 0$$

Study on monetising privacy

An economic model for pricing personal information

The symmetric equilibria in case 1) and 7) are again efficient. The asymmetric equilibria are efficient for intermediate values of q only. For instance in case 2), as the upper bound is larger than $\Delta c(\bar{\theta})$, the equilibrium is inefficient as soon as $q \geq \Delta c(\bar{\theta})$. However, if q is smaller than $\Delta c(\bar{\theta})$ the equilibrium is efficient. In the other cases the asymmetric equilibrium can be inefficient, if q is close to one of the limits.

Scenario a): $\Delta b(\underline{\theta}) > 0 > \Delta b(\bar{\theta})$

We start with the assumption of symmetric data requirements $\bar{d}_A = \bar{d}_B = \bar{d}$ and $\underline{d}_A = \underline{d}_B = \underline{d}$. Here the effect of personalisation is very pronounced as firms would otherwise make second period profits of zero in a symmetric equilibrium. Therefore let us turn to second period profits:

i) Assume first period market shares are $n_{A,1} = n_{B,1} = 0.5$. Then we have to compare the following profits

$$\Pi^1_{B,2} = \tfrac{1}{2}(1-\mu)(p_{A,2}+b+q) \quad ; \quad \Pi^1_{A,2} = (1-\tfrac{1}{2}(1-\mu))(p_{A,2}+q)$$
$$\Pi^2_{B,2} = (1-\tfrac{1}{2}(1-\mu))(p_{A,2}+q) \quad ; \quad \Pi^2_{A,2} = \tfrac{1}{2}(1-\mu)(p_{A,2}+q)$$
$$\Pi^3_{B,2} = p_{A,2}-b+q \quad\quad\quad\quad ; \quad \Pi^3_{A,2} = 0$$

Comparing the profits of firm B, calculating the optimal price $p_{A,2}$ leads to the following profits

$$\Pi^{S1}_{A,2} = \begin{cases} \tfrac{1}{2}b(3-\mu) & \text{if} \quad 1 \geq \mu(6-\mu) \\ \frac{b(1-\mu^2)}{4\mu} & \text{if} \quad \mu(6-\mu)>1 \end{cases} ; \Pi^{S1}_{B,2} = \begin{cases} \frac{2b(1-\mu)}{1+\mu} & \text{if} \quad 1 \geq \mu(6-\mu) \\ \frac{b(1-\mu^2)}{4\mu} & \text{if} \quad \mu(6-\mu)>1 \end{cases}$$

ii) If first period prices are $p_{A,1} < p_{B,1}$, then all consumers buy at firm A in period 1. Thus, second period profits are given by

$$\Pi^1_{B,2} = (p_{A,2}+q)\mu \quad ; \quad \Pi^1_{A,2} = (p_{A,2}+q)(1-\mu)$$
$$\Pi^2_{B,2} = p_{A,2}-b+q \quad ; \quad \Pi^2_{A,2} = 0$$

Therefore, we get

$$\Pi^{S2}_{A,2} = b \text{ and } \Pi^{S2}_{B,2} = \frac{b\mu}{1-\mu}$$

iii) If first period prices are $p_{A,1} > p_{B,1}$, then all consumers buy at firm B in period 1 which leads to

$$\Pi^1_{B,2} = (p_{A,2}+b+q)(1-\mu) \quad ; \quad \Pi^1_{A,2} = (p_{A,2}+q)\mu$$
$$\Pi^2_{B,2} = p_{A,2}+q \quad\quad\quad\quad ; \quad \Pi^2_{A,2} = 0$$

and

$$\Pi^{S3}_{A,2} = b(1-\mu) \text{ and } \Pi^{S3}_{B,2} = b\left(\frac{1}{\mu}-1\right)$$

Note that in all cases no consumer, who has chosen personalisation in the first period, switches in the second period.

Turning to the first period we get the following overall profits

$$
\Pi_B^S = \begin{cases} (p_{A,1}+q)+\Pi_{B,2}^{S3} & \text{if} \quad p_{B,1} < p_{A,1} \\ \frac{1}{2}(p_{A,1}+q)+\Pi_{B,2}^{S1} & \text{if} \quad p_{B,1} = p_{A,1} \\ \Pi_{B,2}^{S2} & \text{if} \quad p_{B,1} > p_{A,1} \end{cases} ; \quad \Pi_A^S = \begin{cases} \Pi_{A,2}^{S3} & \text{if} \quad p_{B,1} < p_{A,1} \\ \frac{1}{2}(p_{A,1}+q)+\Pi_{A,2}^{S1} & \text{if} \quad p_{B,1} = p_{A,1} \\ p_{A,1}+q+\Pi_{A,2}^{S2} & \text{if} \quad p_{B,1} > p_{A,1} \end{cases}
$$

Comparing these profits we again have to consider different cases:

Case 1): $1 \geq \mu(6-\mu)$; Substituting the above given second period profits, overall profits can be written as

$$
\Pi_B = \begin{cases} (p_{A,1}+q)+b\frac{1-\mu}{\mu} & \text{if} \quad p_{B,1} < p_{A,1} \\ \frac{1}{2}(p_{A,1}+q)+\frac{2b(1-\mu)}{1+\mu} & \text{if} \quad p_{B,1} = p_{A,1} \\ b\frac{\mu}{1-\mu} & \text{if} \quad p_{B,1} > p_{A,1} \end{cases} ; \quad \Pi_A = \begin{cases} b(1-\mu) & \text{if} \quad p_{B,1} < p_{A,1} \\ \frac{1}{2}(p_{A,1}+q+b(3-\mu)) & \text{if} \quad p_{B,1} = p_{A,1} \\ p_{A,1}+q+b & \text{if} \quad p_{B,1} > p_{A,1} \end{cases}
$$

Comparing these profits and calculating the best response of firm B and the optimal price $p_{A,1}$ leads to

$$
p_{A,1} = b\frac{2\mu-1}{\mu(1-\mu)} - q
$$

and the following profits

$$
\Pi_A^S = b(1-\mu) \text{ and } \Pi_B^S = b\frac{\mu}{1-\mu}
$$

Case 2): $(6-\mu) > 1$; Again, using the above given second period profits, we get

$$
\Pi_{B,1} = \begin{cases} p_{A,1}+q+b\frac{1-\mu}{\mu} & \text{if} \quad p_{B,1} < p_{A,1} \\ \frac{1}{2}(p_{A,1}+q)+b\frac{1-\mu^2}{4\mu} & \text{if} \quad p_{B,1} = p_{A,1} \\ b\frac{\mu}{1-\mu} & \text{if} \quad p_{B,1} > p_{A,1} \end{cases} ; \quad \Pi_{A,1} = \begin{cases} b(1-\mu) & \text{if} \quad p_{B,1} < p_{A,1} \\ \frac{1}{2}(p_{A,1}+q)+b\frac{1-\mu^2}{4\mu} & \text{if} \quad p_{B,1} = p_{A,1} \\ b\left(1-\frac{1-2\mu}{\mu(1-\mu)}\right) & \text{if} \quad p_{B,1} > p_{A,1} \text{ and } \mu < \frac{1}{3} \\ b\frac{(1+\mu)(\mu(4-\mu)-1)}{2\mu(1-\mu)} & \text{if} \quad p_{B,1} > p_{A,1} \text{ and } \mu \geq \frac{1}{3} \end{cases}
$$

Comparing these profits and calculating the best response of firm B and the optimal price $p_{A,1}$ leads to

$$
p_{A,2} = \begin{cases} b\frac{2\mu-1}{\mu(1-\mu)} - q & \text{if} \quad \mu < \frac{1}{3} \\ b\frac{\mu(1+\mu(5-\mu))-1}{2\mu(1-\mu)} - q & \text{if} \quad \mu > \frac{1}{3} \end{cases}
$$

and the following profits

$$
\Pi_A^S = \begin{cases} b(1-\mu) & \text{if} \quad \mu < \frac{1}{3} \\ b\frac{(1+\mu)(\mu(4-\mu)-1)}{2\mu(1-\mu)} & \text{if} \quad \mu > \frac{1}{3} \end{cases} ; \quad \Pi_B^S = \begin{cases} b\frac{\mu}{1-\mu} & \text{if} \quad \mu < \frac{1}{3} \\ b\frac{\mu}{1-\mu} & \text{if} \quad \mu > \frac{1}{3} \end{cases}
$$

Now, we turn to the case where $d_A = \bar{d} > \underline{d} = d_B$. Again we start with the second period and analyse the firms' profits given different market shares in period 1.

enisa
European Network
and Information
Security Agency

Study on monetising privacy

An economic model for pricing personal information

---

i) If first period market shares were either such that only consumers with $\theta_i = \underline{\theta}$ or all consumers regardless of their type bought from firm A then second period profits are given by:

$$
\begin{aligned}
\Pi^1_{B,2} &:= p_{A,2} - b + \Delta c(\underline{\theta}) \quad ; \quad \Pi^1_{A,2} = 0 \\
\Pi^2_{B,2} &:= (p_{A,2} + \Delta c(\overline{\theta}))\mu \quad ; \quad \Pi^2_{A,2} = (p_{A,2} + q)(1-\mu) \\
\Pi^3_{B,2} &:= 0 \quad\quad\quad\quad\quad\quad ; \quad \Pi^3_{A,2} = -\Delta c(\overline{\theta}) + q
\end{aligned}
$$

The optimal pricing decisions of firm A and the implied profits for both firms are given by

$$
p_{A,2} = \begin{cases}
\frac{\Delta c(\overline{\theta})\mu - \Delta c(\underline{\theta}) + b}{1-\mu} & \text{if} \quad q < \frac{-\mu\Delta c(\overline{\theta}) + \Delta c(\underline{\theta}) - b}{(1-\mu)} \\
\frac{\Delta c(\overline{\theta})\mu - \Delta c(\underline{\theta}) + b}{1-\mu} & \text{if} \quad \frac{(1+\mu)\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) + b}{\mu} \geq q \geq \frac{-\mu\Delta c(\overline{\theta}) + \Delta c(\underline{\theta}) - b}{(1-\mu)} \\
-\Delta c(\overline{\theta}) & \text{if} \quad \frac{(1+\mu)\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) + b}{\mu} < q
\end{cases}
$$

$$
\Pi^{A1}_{A,2} = \begin{cases}
0 & \text{if} \quad q < \frac{-\mu\Delta c(\overline{\theta}) + \Delta c(\underline{\theta}) - b}{(1-\mu)} \\
\Delta c(\overline{\theta})\mu - \Delta c(\underline{\theta}) + b + q(1-\mu) & \text{if} \quad \frac{(1+\mu)\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) + b}{\mu} \geq q \geq \frac{-\mu\Delta c(\overline{\theta}) + \Delta c(\underline{\theta}) - b}{(1-\mu)} \\
-\Delta c(\overline{\theta}) + q & \text{if} \quad \frac{(1+\mu)\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) + b}{\mu} < q
\end{cases}
$$

$$
\Pi^{A1}_{B,2} = \begin{cases}
\frac{\mu}{1-\mu}\left(\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) + b\right) & \text{if} \quad q < \frac{-\mu\Delta c(\overline{\theta}) + \Delta c(\underline{\theta}) - b}{(1-\mu)} \\
\frac{\mu}{1-\mu}\left(\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) + b\right) & \text{if} \quad \frac{(1+\mu)\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) + b}{\mu} \geq q \geq \frac{-\mu\Delta c(\overline{\theta}) + \Delta c(\underline{\theta}) - b}{(1-\mu)} \\
0 & \text{if} \quad \frac{(1+\mu)\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) + b}{\mu} < q
\end{cases}
$$

ii) If in contrast all consumers bought from firm B in the first period, second period profits are given by

$$
\begin{aligned}
\Pi^1_{B,2} &:= p_{A,2} + b + \Delta c(\underline{\theta}) \quad ; \quad \Pi^1_{A,2} = 0 \\
\Pi^2_{B,2} &:= (p_{A,2} + \Delta c(\overline{\theta}))\mu \quad ; \quad \Pi^2_{A,2} = (p_{A,2} + q)(1-\mu) \\
\Pi^3_{B,2} &:= 0 \quad\quad\quad\quad\quad\quad ; \quad \Pi^3_{A,2} = (-b - \Delta c(\underline{\theta}) + q)
\end{aligned}
$$

Prices and profits are given by

$$
p_{A,2} = \begin{cases}
\frac{\Delta c(\overline{\theta})\mu - \Delta c(\underline{\theta}) - b}{1-\mu} & \text{if} \quad b + \Delta c(\underline{\theta}) > q \\
-b - \Delta c(\underline{\theta}) & \text{if} \quad b + \Delta c(\underline{\theta}) < q
\end{cases} ;
$$

$$
\Pi^{A2}_{A,2} = \begin{cases}
0 & \text{if} \quad b + \Delta c(\underline{\theta}) > q \\
-b - \Delta c(\underline{\theta}) + q & \text{if} \quad b + \Delta c(\underline{\theta}) < q
\end{cases} ;
$$

$$
\Pi^{A2}_{B,2} = \begin{cases}
\frac{\mu}{1-\mu}\left(\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) - b\right) & \text{if} \quad b + \Delta c(\underline{\theta}) > q \\
0 & \text{if} \quad b + \Delta c(\underline{\theta}) < q
\end{cases}
$$

Now, we turn to the first period pricing decisions when data requirements are asymmetric. We get the following overall profits:

Study on monetising privacy

An economic model for pricing personal information

$$\Pi_B = \begin{cases} \Pi_{B,2}^{A1} & \text{if} \quad p_{B,1} \geq p_{A,1} + \Delta c\!\left(\overline{\theta}\right) \\ \mu\!\left(p_{A1} + \Delta c\!\left(\overline{\theta}\right)\right) + \Pi_{B,2}^{A1} & \text{if} \quad p_{A,1} + \Delta c\!\left(\underline{\theta}\right) \leq p_{B,1} < p_{A,1} + \Delta c\!\left(\overline{\theta}\right) \\ p_{A,1} + \Delta c\!\left(\underline{\theta}\right) + \Pi_{B,2}^{A2} & \text{if} \quad p_{B,1} < p_{A,1} + \Delta c\!\left(\underline{\theta}\right) \end{cases}$$

$$\Pi_A = \begin{cases} p_{A1} + q + \Pi_{A,2}^{A1} & \text{if} \quad p_{B,1} \geq p_{A,1} + \Delta c\!\left(\overline{\theta}\right) \\ (1-\mu)\!\left(p_{A1} + q\right) + \Pi_{A,2}^{A1} & \text{if} \quad p_{A,1} + \Delta c\!\left(\underline{\theta}\right) \leq p_{B,1} < p_{A,1} + \Delta c\!\left(\overline{\theta}\right) \\ \Pi_{A,2}^{A2} & \text{if} \quad p_{B,1} < p_{A,1} + \Delta c\!\left(\underline{\theta}\right) \end{cases}$$

In order to analyse the firms' decisions we again have to distinguish different cases concerning the value of q.

Case 1): $q < \frac{-\mu \Delta c\!\left(\overline{\theta}\right) + \Delta c\!\left(\underline{\theta}\right) - b}{(1-\mu)}$; This leads to

$$\Pi_B = \begin{cases} \mu\!\left(p_{A,1} + \Delta c\!\left(\overline{\theta}\right)\right) + \frac{\mu}{1-\mu}\!\left(\Delta c\!\left(\overline{\theta}\right) - \Delta c\!\left(\underline{\theta}\right) + b\right) & \text{if} \quad p_{A,1} + \Delta c\!\left(\underline{\theta}\right) \leq p_{B,1} < p_{A,1} + \Delta c\!\left(\overline{\theta}\right) \\ \frac{\mu}{1-\mu}\!\left(\Delta c\!\left(\overline{\theta}\right) - \Delta c\!\left(\underline{\theta}\right) + b\right) & \text{if} \quad p_{B,1} \geq p_{A,1} + \Delta c\!\left(\overline{\theta}\right) \\ p_{A,1} + \Delta c\!\left(\underline{\theta}\right) + \frac{\mu}{1-\mu}\!\left(\Delta c\!\left(\overline{\theta}\right) - \Delta c\!\left(\underline{\theta}\right) - b\right) & \text{if} \quad p_{B,1} < p_{A,1} + \Delta c\!\left(\underline{\theta}\right) \end{cases}$$

$$\Pi_A = \begin{cases} (1-\mu)\!\left(p_{A,1} + q\right) & \text{if} \quad p_{A,1} + \Delta c\!\left(\underline{\theta}\right) \leq p_{B,1} < p_{A,1} + \Delta c\!\left(\overline{\theta}\right) \\ q - \Delta c\!\left(\overline{\theta}\right) & \text{if} \quad p_{B,1} \geq p_{A,1} + \Delta c\!\left(\overline{\theta}\right) \\ 0 & \text{if} \quad p_{B,1} < p_{A,1} + \Delta c\!\left(\underline{\theta}\right) \end{cases}$$

Solving for firm A 's price and plugging back into the profit functions yields

$$p_{A,1} = \frac{\mu}{(1-\mu)^2} 2b + \frac{1}{1-\mu}\!\left(\mu \Delta c\!\left(\overline{\theta}\right) - \Delta c\!\left(\underline{\theta}\right)\right)$$

$$\Pi_A^{AA} = \begin{cases} 0 & \text{if} \quad q < -\frac{\mu}{(1-\mu)^2} 2b + \frac{1}{1-\mu}\!\left(\mu \Delta c\!\left(\overline{\theta}\right) + \Delta c\!\left(\underline{\theta}\right)\right) \\ \frac{\mu}{(1-\mu)} 2b + \mu \Delta c\!\left(\overline{\theta}\right) - \Delta c\!\left(\underline{\theta}\right) + (1-\mu)q & \text{if} \quad q > -\frac{\mu}{(1-\mu)^2} 2b + \frac{1}{1-\mu}\!\left(\mu \Delta c\!\left(\overline{\theta}\right) + \Delta c\!\left(\underline{\theta}\right)\right) \end{cases}$$

$$\Pi_B^{AA} = \frac{\mu}{(1-\mu)^2}\!\left(2\!\left(\Delta c\!\left(\overline{\theta}\right) - \Delta c\!\left(\underline{\theta}\right)\right)(1-\mu) + b(1+\mu)\right)$$

Case 2): $b + \Delta c\!\left(\overline{\theta}\right) \geq q \geq \frac{-\mu \Delta c\!\left(\overline{\theta}\right) + \Delta c\!\left(\underline{\theta}\right) - b}{(1-\mu)}$; Now, profits are

$$\Pi_B = \begin{cases} \mu\!\left(p_{A1} + \Delta c\!\left(\overline{\theta}\right)\right) + \frac{\mu}{1-\mu}\!\left(\Delta c\!\left(\overline{\theta}\right) - \Delta c\!\left(\underline{\theta}\right) + b\right) & \text{if} \quad p_{A,1} + \Delta c\!\left(\underline{\theta}\right) \leq p_{B,1} < p_{A,1} + \Delta c\!\left(\overline{\theta}\right) \\ \frac{\mu}{1-\mu}\!\left(\Delta c\!\left(\overline{\theta}\right) - \Delta c\!\left(\underline{\theta}\right) + b\right) & \text{if} \quad p_{B,1} \geq p_{A,1} + \Delta c\!\left(\overline{\theta}\right) \\ p_{A,1} + \Delta c\!\left(\underline{\theta}\right) + \frac{\mu}{1-\mu}\!\left(\Delta c\!\left(\overline{\theta}\right) - \Delta c\!\left(\underline{\theta}\right) - b\right) & \text{if} \quad p_{B,1} < p_{A,1} + \Delta c\!\left(\underline{\theta}\right) \end{cases}$$

$$\Pi_A = \begin{cases} (1-\mu)\!\left(p_{A1} + q\right) + \Delta c\!\left(\overline{\theta}\right)\mu - \Delta c\!\left(\underline{\theta}\right) + b + q(1-\mu) & \text{if} \quad p_{A,1} + \Delta c\!\left(\underline{\theta}\right) \leq p_{B,1} < p_{A,1} + \Delta c\!\left(\overline{\theta}\right) \\ -\Delta c\!\left(\overline{\theta}\right) + q + \Delta c\!\left(\overline{\theta}\right)\mu - \Delta c\!\left(\underline{\theta}\right) + b + q(1-\mu) & \text{if} \quad p_{B,1} \geq p_{A,1} + \Delta c\!\left(\overline{\theta}\right) \\ 0 & \text{if} \quad p_{B,1} < p_{A,1} + \Delta c\!\left(\underline{\theta}\right) \end{cases}$$

Then, we get:

enisa
European Network
and Information
Security Agency

Study on monetising privacy

An economic model for pricing personal information

$$p_{A,1} = \frac{\mu}{(1-\mu)^2} 2b + \frac{1}{1-\mu}\left(\mu\Delta c(\overline{\theta}) - \Delta c(\underline{\theta})\right)$$

$$\Pi_A^{AA} = \begin{cases} 0 & \text{if} \quad q < -\frac{1}{2(1-\mu)^2}\left(b(1+\mu) + 2(1-\mu)\left(\mu\Delta c(\overline{\theta}) - \Delta c(\underline{\theta})\right)\right) \\ \frac{1+\mu}{(1-\mu)}b + 2\left(\mu\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) + (1-\mu)q\right) & \text{if} \quad q > -\frac{1}{2(1-\mu)^2}\left(b(1+\mu) + 2(1-\mu)\left(\mu\Delta c(\overline{\theta}) - \Delta c(\underline{\theta})\right)\right) \end{cases}$$

$$\Pi_B^{AA} = \frac{\mu}{(1-\mu)^2}\left(2\left(\Delta c(\overline{\theta}) - \Delta c(\underline{\theta})\right)(1-\mu) + b(1+\mu)\right)$$

Case 3): $\frac{(1+\mu)\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) + b}{\mu} \geq q > b + \Delta c(\overline{\theta})$; For these values of q, we have the following profits:

$$\Pi_B = \begin{cases} \mu\left(p_{A1} + \Delta c(\overline{\theta})\right) + \frac{\mu}{1-\mu}\left(\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) + b\right) & \text{if} \quad p_{A,1} + \Delta c(\underline{\theta}) \leq p_{B,1} < p_{A,1} + \Delta c(\overline{\theta}) \\ \frac{\mu}{1-\mu}\left(\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) + b\right) & \text{if} \quad p_{B,1} \geq p_{A,1} + \Delta c(\overline{\theta}) \\ p_{A,1} + \Delta c(\underline{\theta}) & \text{if} \quad p_{B,1} < p_{A,1} + \Delta c(\underline{\theta}) \end{cases}$$

$$\Pi_A = \begin{cases} (1-\mu)\left(p_{A1} + q\right) + \mu\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) + (1-\mu)q + b & \text{if} \quad p_{A,1} + \Delta c(\underline{\theta}) \leq p_{B,1} < p_{A,1} + \Delta c(\overline{\theta}) \\ -\Delta c(\overline{\theta}) + q + \Delta c(\overline{\theta})\mu - \Delta c(\underline{\theta}) + b + q(1-\mu) & \text{if} \quad p_{B,1} \geq p_{A,1} + \Delta c(\overline{\theta}) \\ -b - \Delta c(\underline{\theta}) + q & \text{if} \quad p_{B,1} < p_{A,1} + \Delta c(\underline{\theta}) \end{cases}$$

These profits lead to

$$p_{A1} = -\Delta c(\overline{\theta})$$

$$\Pi_B^{AA} = \frac{\mu}{1-\mu}\left(\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) + b\right)$$

$$\Pi_A^{AA} = -\Delta c(\overline{\theta}) + q + \Delta c(\overline{\theta})\mu - \Delta c(\underline{\theta}) + b + q(1-\mu)$$

Case 4): $b + \Delta c(\overline{\theta}) > q$; In this case, profits are

$$\Pi_B = \begin{cases} \mu\left(p_{A1} + \Delta c(\overline{\theta})\right) & \text{if} \quad p_{A,1} + \Delta c(\underline{\theta}) \leq p_{B,1} < p_{A,1} + \Delta c(\overline{\theta}) \\ 0 & \text{if} \quad p_{B,1} \geq p_{A,1} + \Delta c(\overline{\theta}) \\ p_{A,1} + \Delta c(\underline{\theta}) & \text{if} \quad p_{B,1} < p_{A,1} + \Delta c(\underline{\theta}) \end{cases}$$

$$\Pi_A = \begin{cases} (1-\mu)\left(p_{A1} + q\right) - \Delta c(\overline{\theta}) + q & \text{if} \quad p_{A,1} + \Delta c(\underline{\theta}) \leq p_{B,1} < p_{A,1} + \Delta c(\overline{\theta}) \\ 2\left(q - \Delta c(\overline{\theta})\right) & \text{if} \quad p_{B,1} \geq p_{A,1} + \Delta c(\overline{\theta}) \\ -b - \Delta c(\underline{\theta}) + q & \text{if} \quad p_{B,1} < p_{A,1} + \Delta c(\underline{\theta}) \end{cases}$$

Prices and profits are given by:

$$p_{A,1} = -\Delta c(\overline{\theta}); \Pi_{B,1}^{AA} = 0 \text{ and } \Pi_{A,1}^{AA} = 2\left(q - \Delta c(\overline{\theta})\right)$$

Finally, assume $d_B = \overline{d} > \underline{d} = d_A$. We proceed as in the previous case.

i) If first period market shares were either such that only consumers with $\theta = \overline{\theta}$ or all consumers regardless of their type bought from firm B we get the following scheme

$$\Pi^1_{B,2} := p_{A,2} + q - \Delta c(\bar\theta) \qquad ; \quad \Pi^1_{A,2} = 0$$
$$\Pi^2_{B,2} := (p_{A,2} + q + b - \Delta c(\underline\theta))(1-\mu) \quad ; \quad \Pi^2_{A,2} = p_{A,2}\mu$$
$$\Pi^3_{B,2} := 0 \qquad ; \quad \Pi^3_{A,2} = \Delta c(\underline\theta) - b - q$$

This leads to the following second period outcomes

$$p_{A,2} = \begin{cases} \frac{\Delta c(\bar\theta) - (1-\mu)\Delta c(\underline\theta) + (1-\mu)b - \mu q}{\mu} & \text{if} \quad q > \frac{-(1-\mu)(\Delta c(\underline\theta) - b) + \Delta c(\bar\theta)}{\mu} \\ \frac{\Delta c(\bar\theta) - (1-\mu)\Delta c(\underline\theta) + (1-\mu)b - \mu q}{\mu} & \text{if} \quad \frac{-(1-\mu)(\Delta c(\underline\theta) - b) + \Delta c(\bar\theta)}{\mu} \ge q \ge \frac{(2-\mu)(\Delta c(\underline\theta) - b) - \Delta c(\bar\theta)}{1-\mu} \\ \Delta c(\underline\theta) - b - q & \text{if} \quad \frac{(2-\mu)(\Delta c(\underline\theta) - b) - \Delta c(\bar\theta)}{1-\mu} > q \end{cases}$$

$$\Pi^{A3}_{A,2} = \begin{cases} 0 & \text{if} \quad q > \frac{-(1-\mu)(\Delta c(\underline\theta) - b) + \Delta c(\bar\theta)}{\mu} \\ \Delta c(\bar\theta) - (1-\mu)(\Delta c(\underline\theta) - b) - \mu q & \text{if} \quad \frac{-(1-\mu)(\Delta c(\underline\theta) - b) + \Delta c(\bar\theta)}{\mu} \ge q \ge \frac{(2-\mu)(\Delta c(\underline\theta) - b) - \Delta c(\bar\theta)}{1-\mu} \\ \Delta c(\underline\theta) - b - q & \text{if} \quad \frac{(2-\mu)(\Delta c(\underline\theta) - b) - \Delta c(\bar\theta)}{1-\mu} > q \end{cases}$$

$$\Pi^{A3}_{B,2} = \begin{cases} \frac{1-\mu}{\mu}\left(b - \Delta c(\underline\theta) + \Delta c(\bar\theta)\right) & \text{if} \quad q > \frac{-(1-\mu)(\Delta c(\underline\theta) - b) + \Delta c(\bar\theta)}{\mu} \\ \frac{1-\mu}{\mu}\left(b - \Delta c(\underline\theta) + \Delta c(\bar\theta)\right) & \text{if} \quad \frac{-(1-\mu)(\Delta c(\underline\theta) - b) + \Delta c(\bar\theta)}{\mu} \ge q \ge \frac{(2-\mu)(\Delta c(\underline\theta) - b) - \Delta c(\bar\theta)}{1-\mu} \\ 0 & \text{if} \quad \frac{(2-\mu)(\Delta c(\underline\theta) - b) - \Delta c(\bar\theta)}{1-\mu} > q \end{cases}$$

ii) If all consumers bought from firm A in the first period we get

$$\Pi^1_{B,2} := p_{A,2} + q - \Delta c(\bar\theta) \qquad ; \quad \Pi^1_{A,2} = 0$$
$$\Pi^2_{B,2} := (p_{A,2} + q - b - \Delta c(\underline\theta))(1-\mu) \quad ; \quad \Pi^2_{A,2} = p_{A,2}\mu$$
$$\Pi^3_{B,2} := 0 \qquad ; \quad \Pi^3_{A,2} = \Delta c(\bar\theta) - q$$

And thus

$$p_{A,2} = \begin{cases} \frac{\Delta c(\bar\theta) - (1-\mu)(\Delta c(\underline\theta) + b) - \mu q}{\mu} & \text{if} \quad q > b + \Delta c(\underline\theta) \\ \Delta c(\bar\theta) - q & \text{if} \quad q < b + \Delta c(\underline\theta) \end{cases}$$

$$\Pi^{A4}_{A,2} = \begin{cases} 0 & \text{if} \quad q > b + \Delta c(\underline\theta) \\ \Delta c(\bar\theta) - q & \text{if} \quad q < b + \Delta c(\underline\theta) \end{cases}$$

$$\Pi^{A4}_{B,2} = \begin{cases} \frac{(1-\mu)}{\mu}\left(\left(\Delta c(\bar\theta) - \Delta c(\underline\theta) - b\right)\right) & \text{if} \quad q > b + \Delta c(\underline\theta) \\ 0 & \text{if} \quad q < b + \Delta c(\underline\theta) \end{cases}$$

Turning to the first period, profits and prices are given by:

$$\Pi_B = \begin{cases} \Pi^{A4}_{B,2} & \text{if} \quad p_{B,1} \ge p_{A,1} - \Delta c(\underline\theta) \\ (1-\mu)\left(p_{A,1} - \Delta c(\underline\theta) + q\right) + \Pi^{A3}_{B,2} & \text{if} \quad p_{A,1} - \Delta c(\bar\theta) \le p_{B,1} < p_{A,1} - \Delta c(\underline\theta) \\ p_{A,1} - \Delta c(\bar\theta) + q + \Pi^{A3}_{B,2} & \text{if} \quad p_{B,1} < p_{A,1} - \Delta c(\bar\theta) \end{cases}$$

$$\Pi_A = \begin{cases} p_{A1} + \Pi^{A4}_{A,2} & \text{if} \quad p_{B,1} \ge p_{A,1} - \Delta c(\underline\theta) \\ \mu p_{A1} + \Pi^{A3}_{A,2} & \text{if} \quad p_{A,1} - \Delta c(\bar\theta) \le p_{B,1} < p_{A,1} - \Delta c(\underline\theta) \\ \Pi^{A3}_{A,2} & \text{if} \quad p_{B,1} < p_{A,1} - \Delta c(\bar\theta) \end{cases}$$

enisa European Network and Information Security Agency

Study on monetising privacy

An economic model for pricing personal information

Again, we have to consider different parameter constellations:

Case 1): $q < \frac{(2-\mu)(\Delta c(\underline{\theta})-b)-\Delta c(\bar{\theta})}{1-\mu}$; Analysing the profit functions

$$\Pi_B = \begin{cases} (1-\mu)\big(p_{A,1} - \Delta c(\underline{\theta}) + q\big) & \text{if} \quad p_{A,1} - \Delta c(\bar{\theta}) \le p_{B,1} < p_{A,1} - \Delta c(\underline{\theta}) \\ 0 & \text{if} \quad p_{B,1} \ge p_{A,1} - \Delta c(\underline{\theta}) \\ p_{A,1} - \Delta c(\bar{\theta}) + q & \text{if} \quad p_{B,1} < p_{A,1} - \Delta c(\bar{\theta}) \end{cases}$$

$$\Pi_A = \begin{cases} \mu p_{A1} + \Delta c(\underline{\theta}) - b - q & \text{if} \quad p_{A,1} - \Delta c(\bar{\theta}) \le p_{B,1} < p_{A,1} - \Delta c(\underline{\theta}) \\ \Delta c(\bar{\theta}) + \Delta c(\underline{\theta}) - 2q & \text{if} \quad p_{B,1} \ge p_{A,1} - \Delta c(\underline{\theta}) \\ \Delta c(\underline{\theta}) - b - q & \text{if} \quad p_{B,1} < p_{A,1} - \Delta c(\bar{\theta}) \end{cases}$$

leads to the following price $p_{A,1}$ and overall profits

$$p_{A,1} = \Delta c(\underline{\theta}) - q$$
$$\Pi_{A,1}^{AB} = \Delta c(\bar{\theta}) + \Delta c(\underline{\theta}) - 2q \text{ and } \Pi_{B,1}^{AB} = 0$$

Case 2): $b + \Delta c(\underline{\theta}) > q > \frac{(2-\mu)(\Delta c(\underline{\theta})-b)-\Delta c(\bar{\theta})}{1-\mu}$; In this case we have

$$\Pi_B = \begin{cases} (1-\mu)\big(p_{A,1} - \Delta c(\underline{\theta}) + q\big) + \frac{1-\mu}{\mu}\big(b - \Delta c(\bar{\theta}) + \Delta c(\underline{\theta})\big) & \text{if} \quad p_{A,1} - \Delta c(\bar{\theta}) \le p_{B,1} < p_{A,1} - \Delta c(\underline{\theta}) \\ 0 & \text{if} \quad p_{B,1} \ge p_{A,1} - \Delta c(\underline{\theta}) \\ p_{A,1} - \Delta c(\bar{\theta}) + q + \frac{1-\mu}{\mu}\big(b - \Delta c(\bar{\theta}) + \Delta c(\underline{\theta})\big) & \text{if} \quad p_{B,1} < p_{A,1} - \Delta c(\bar{\theta}) \end{cases}$$

$$\Pi_A = \begin{cases} \mu p_{A1} + \Delta c(\bar{\theta}) - (1-\mu)\big(\Delta c(\underline{\theta}) - b\big) - \mu q & \text{if} \quad p_{A,1} - \Delta c(\bar{\theta}) \le p_{B,1} < p_{A,1} - \Delta c(\underline{\theta}) \\ \frac{1}{\mu}\big(-b + \Delta c(\bar{\theta})(1+\mu) - \Delta c(\underline{\theta})(1-\mu)\big) - 2q & \text{if} \quad p_{B,1} \ge p_{A,1} - \Delta c(\underline{\theta}) \\ \Delta c(\bar{\theta}) - (1-\mu)\big(\Delta c(\underline{\theta}) - b\big) - \mu q & \text{if} \quad p_{B,1} < p_{A,1} - \Delta c(\bar{\theta}) \end{cases}$$

The optimal price $p_{A,1}$ and the firms' profits are given by

$$p_{A,1} = \begin{cases} -\frac{1}{\mu}b + \frac{1}{\mu}\big(\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})(1-\mu)\big) - q & \text{if} \quad q < \frac{1}{2\mu(1-\mu)}\big((1-\mu)\big(\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})(1-2\mu)\big) - b\big(1+\mu-\mu^2\big)\big) \\ \frac{1}{\mu}\big(\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})(1-\mu)\big) - q & \text{if} \quad q > \frac{1}{2\mu(1-\mu)}\big((1-\mu)\big(\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})(1-2\mu)\big) - b\big(1+\mu-\mu^2\big)\big) \end{cases}$$

$$\Pi_A^{AB} = \begin{cases} \frac{1}{\mu}\big(-b + \Delta c(\bar{\theta})(1+\mu) - \Delta c(\underline{\theta})(1-\mu)\big) - 2q & \text{if} \quad q < \frac{1}{2\mu(1-\mu)}\big((1-\mu)\big(\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})(1-2\mu)\big) - b\big(1+\mu-\mu^2\big)\big) \\ \big(b - 2\Delta c(\underline{\theta})\big)(1-\mu) + 2\big(\Delta c(\bar{\theta}) - \mu q\big) & \text{if} \quad q > \frac{1}{2\mu(1-\mu)}\big((1-\mu)\big(\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})(1-2\mu)\big) - b\big(1+\mu-\mu^2\big)\big) \end{cases}$$

$$\Pi_B^{AB} = \begin{cases} 0 & \text{if} \quad q < \frac{1}{2\mu(1-\mu)}\big((1-\mu)\big(\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})(1-2\mu)\big) - b\big(1+\mu-\mu^2\big)\big) \\ b\frac{1-\mu}{\mu} & \text{if} \quad q > \frac{1}{2\mu(1-\mu)}\big((1-\mu)\big(\Delta c(\bar{\theta}) - \Delta c(\underline{\theta})(1-2\mu)\big) - b\big(1+\mu-\mu^2\big)\big) \end{cases}$$

Case 3): $\frac{-(1-\mu)(\Delta c(\underline{\theta})-b)+\Delta c(\bar{\theta})}{\mu} > q > b + \Delta c(\underline{\theta})$; Profits can be written as

$$\Pi_B = \begin{cases} (1-\mu)\left(p_{A,1} - \Delta c(\underline{\theta}) + q\right) + \frac{1-\mu}{\mu}\left(\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) + b\right) & \text{if} \quad p_{A,1} - \Delta c(\overline{\theta}) \le p_{B,1} < p_{A,1} - \Delta c(\underline{\theta}) \\ \frac{1-\mu}{\mu}\left(\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) - b\right) & \text{if} \quad p_{B,1} \ge p_{A,1} - \Delta c(\underline{\theta}) \\ p_{A,1} - \Delta c(\overline{\theta}) + q + \frac{1-\mu}{\mu}\left(\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) + b\right) & \text{if} \quad p_{B,1} < p_{A,1} - \Delta c(\overline{\theta}) \end{cases}$$

$$\Pi_A = \begin{cases} \mu p_{A1} + \Delta c(\overline{\theta}) - (1-\mu)\left(\Delta c(\underline{\theta}) - b\right) - \mu q & \text{if} \quad p_{A,1} - \Delta c(\overline{\theta}) \le p_{B,1} < p_{A,1} - \Delta c(\underline{\theta}) \\ \Delta c(\underline{\theta}) - \frac{2b}{\mu} - q & \text{if} \quad p_{B,1} \ge p_{A,1} - \Delta c(\underline{\theta}) \\ \Delta c(\overline{\theta}) - (1-\mu)\left(\Delta c(\underline{\theta}) - b\right) - \mu q & \text{if} \quad p_{B,1} < p_{A,1} - \Delta c(\overline{\theta}) \end{cases}$$

The implied pricing decision of firm A and the firms' profits are given by

$$p_{A,1} = \frac{1}{\mu}\left(\Delta c(\overline{\theta}) - \Delta c(\underline{\theta})(1-\mu)\right) - q$$

$$\Pi_A^{A\overline{B}} = \begin{cases} \left(b - 2\Delta c(\underline{\theta})\right)(1-\mu) + 2\left(\Delta c(\overline{\theta}) - \mu q\right) & \text{if} \quad q < \frac{1}{\mu}\left(\Delta c(\overline{\theta}) - \Delta c(\underline{\theta})(1-\mu)\right) \\ \Delta c(\overline{\theta}) - (1-\mu)\left(\Delta c(\underline{\theta}) - b\right) - \mu q & \text{if} \quad q > \frac{1}{\mu}\left(\Delta c(\overline{\theta}) - \Delta c(\underline{\theta})(1-\mu)\right) \end{cases}$$

$$\Pi_B^{A\overline{B}} = \frac{1-\mu}{\mu}\left(b + 2\left(\Delta c(\overline{\theta}) - \Delta c(\underline{\theta})\right)\right)$$

Case 4): $\frac{-(1-\mu)(\Delta c(\underline{\theta}) - b) + \Delta c(\overline{\theta})}{\mu} < q$; In this final case, we obtain

$$\Pi_B = \begin{cases} (1-\mu)\left(p_{A,1} - \Delta c(\underline{\theta}) + q\right) + \frac{1-\mu}{\mu}\left(\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) + b\right) & \text{if} \quad p_{A,1} - \Delta c(\overline{\theta}) \le p_{B,1} < p_{A,1} - \Delta c(\underline{\theta}) \\ \frac{1-\mu}{\mu}\left(\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) - b\right) & \text{if} \quad p_{B,1} \ge p_{A,1} - \Delta c(\underline{\theta}) \\ p_{A,1} - \Delta c(\overline{\theta}) + q + \frac{1-\mu}{\mu}\left(\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) + b\right) & \text{if} \quad p_{B,1} < p_{A,1} - \Delta c(\overline{\theta}) \end{cases}$$

$$\Pi_A = \begin{cases} \mu p_{A1} & \text{if} \quad p_{A,1} - \Delta c(\overline{\theta}) \le p_{B,1} < p_{A,1} - \Delta c(\underline{\theta}) \\ \Delta c(\underline{\theta}) - q - \frac{2b}{\mu} & \text{if} \quad p_{B,1} \ge p_{A,1} - \Delta c(\underline{\theta}) \\ 0 & \text{if} \quad p_{B,1} < p_{A,1} - \Delta c(\overline{\theta}) \end{cases}$$

As well as

$$p_{A,1} = \frac{1}{\mu}\left(\Delta c(\overline{\theta}) - \left(\Delta c(\underline{\theta}) - q\right)(1-\mu)\right)$$

$$\Pi_A^{A\overline{B}} = 0 \text{ and } \Pi_B^{A\overline{B}} = \frac{1-\mu}{\mu}\left(b + 2\left(\Delta c(\overline{\theta}) - \Delta c(\underline{\theta})\right) + q\right)$$

With all these different cases in mind, we now turn to the firms' data requirement decisions, which are made at the beginning of the first period. To make the model more tractable we derive these decisions for a couple of different parameter values which feature the characteristic results, instead of the whole range of parameters.

We start with an intermediate value of $\mu = 0.5$. Under this assumption, a choice of $d_A = \overline{d}$

leads to the following comparison for firm B 's profits:

$$q \le 3\Delta c(\overline{\theta}) - 2\Delta c(\underline{\theta}) + 2b \quad : \quad \Pi_B^{AA} \ge \Pi_B^{S} \quad \rightarrow d_B = \underline{d}$$
$$q > 3\Delta c(\overline{\theta}) - 2\Delta c(\underline{\theta}) + 2b \quad : \quad \Pi_B^{AA} \le \Pi_B^{S} \quad \rightarrow d_B = \overline{d}$$

Study on monetising privacy

An economic model for pricing personal information

In contrast, $d_A = \underline{d}$ implies that we have a symmetric equilibrium for low values of q only:

$$q \le b + \Delta c(\underline{\theta}) \quad : \quad \Pi_B^{AS} \ge \Pi_B^{AA} \quad \to d_B = \underline{d}$$
$$q > b + \Delta c(\underline{\theta}) \quad : \quad \Pi_B^{AA} \le \Pi_B^{S} \quad \to d_B = \overline{d}$$

Considering the decision of firm A and evaluating the firms' profits for all parameter constellations we get

$$1)\, q < 3\Delta c(\overline{\theta}) - 2\Delta c(\underline{\theta}) - 2b$$
$$\to d_A = \underline{d} \to d_B = \underline{d} \to \Pi_A = 3b$$
$$2)\, 2\Delta c(\underline{\theta}) - \Delta c(\overline{\theta}) - 2b \ge q \ge 3\Delta c(\overline{\theta}) - 2\Delta c(\underline{\theta}) - 2b$$
$$\to d_A = \underline{d} \to d_B = \underline{d} \to \Pi_A = 3b$$
$$3)\, 2\Delta c(\underline{\theta}) - \Delta c(\overline{\theta}) \ge q \ge 2\Delta c(\underline{\theta}) - \Delta c(\overline{\theta}) - 2b$$
$$\to d_A = \underline{d} \to d_B = \underline{d} \to \Pi_A = 3b$$
$$4)\, b + \Delta c(\underline{\theta}) \ge q \ge 2\Delta c(\underline{\theta}) - \Delta c(\overline{\theta})$$
$$\to d_A = \overline{d} \to d_B = \underline{d} \to \Pi_A = 3b + \Delta c(\overline{\theta}) - 2\Delta c(\underline{\theta}) + q$$
$$5)\, b + \Delta c(\overline{\theta}) \ge q \ge b + \Delta c(\underline{\theta})$$
$$\to d_A = \overline{d} \to d_B = \underline{d} \to \Pi_A = 3b + c(\overline{\theta}) - 2\Delta c(\underline{\theta}) + q$$
$$6)\, b + 2\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) \ge q \ge b + \Delta c(\overline{\theta})$$
$$\to d_A = \overline{d} \to d_B = \underline{d} \to \Pi_A = -\frac{1}{2}\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) + b + \frac{3}{2}q$$
$$7)\, 3\Delta c(\overline{\theta}) - 2\Delta c(\underline{\theta}) + 2b \ge q \ge b + 2\Delta c(\overline{\theta}) - \Delta c(\underline{\theta})$$
$$\to d_A = \overline{d} \to d_B = \underline{d} \to \Pi_A = -\frac{1}{2}\Delta c(\overline{\theta}) - \Delta c(\underline{\theta}) + b + \frac{3}{2}q$$
$$8)\, 3\Delta c(\overline{\theta}) - 2\Delta c(\underline{\theta} + 2b < q$$
$$\to d_A = \overline{d} \to d_B = \overline{d} \to \Pi_A = 3b$$

As a second parameterisation of the model we choose $\mu = \frac{1}{4}, \Delta c(\overline{\theta}) = \frac{2}{3}$ and $\Delta c(\underline{\theta}) = \frac{1}{3}$. Starting with $d_A = \overline{d}$ and analysing firm B's best response we get

$$q \le \tfrac{1}{2} + 4b \quad : \quad d_B = \underline{d}$$
$$q > \tfrac{1}{2} + 4b \quad : \quad d_B = \overline{d}$$

Again, equilibrium candidates are asymmetric, except for sufficiently high q. With $d_A = \underline{d}$ we obtain

$$q \le 1 - \tfrac{19}{6}b \quad : \quad d_B = \underline{d}$$
$$q > \tfrac{1}{2} + 4b \quad : \quad d_B = \overline{d}$$

Thus, all possible equilibria are asymmetric, except for the case in which if q is sufficiently low. Assuming different values of b and q leads to the following results:

$$b = \tfrac{1}{2},\ q = 0 \quad : \quad d_A = \overline{d} \quad d_B = \underline{d} \quad \Pi_A^{AA} = \tfrac{1}{2} \quad \Pi_{B,1}^{AA} = \tfrac{1}{2}$$

$$b = 1,\ q = 0 \quad : \quad d_A = \underline{d} \quad d_B = \overline{d} \quad \Pi_A^{AB} = \tfrac{19}{12} \quad \Pi_B^{AB} = 3$$

$$b = \tfrac{1}{2},\ q = \tfrac{1}{2} \quad : \quad d_A = \overline{d} \quad d_B = \underline{d} \quad \Pi_A^{AA} = \tfrac{5}{4} \quad \Pi_B^{AA} = \tfrac{1}{2}$$

$$b = 1,\ q = \tfrac{1}{2} \quad : \quad d_A = \overline{d} \quad d_B = \underline{d} \quad \Pi_{A,1}^{AA} = \tfrac{5}{4} \quad \Pi_B^{AA} = \tfrac{7}{9}$$

$$b = \tfrac{1}{2},\ q = 1 \quad : \quad d_A = \overline{d} \quad d_B = \underline{d} \quad \Pi_A^{AA} = 2 \quad \Pi_B^{AA} = \tfrac{1}{2}$$

$$b = 1,\ q = 1 \quad : \quad d_A = \overline{d} \quad d_B = \underline{d} \quad \Pi_A^{AA} = \tfrac{17}{6} \quad \Pi_B^{AA} = \tfrac{7}{9}$$

As a third parameterisation we consider $\mu = \tfrac{3}{4}, \Delta c(\overline{\theta}) = \tfrac{2}{3}$ and $\Delta c(\underline{\theta}) = \tfrac{1}{3}$. Again considering

different values of b and q we get the following equilibria

$$b = \tfrac{1}{2},\ q = 0 \quad : \quad d_A = \overline{d} \quad d_B = \underline{d} \quad \Pi_A^{AA} = \tfrac{23}{6} \quad \Pi_B^{AA} = \tfrac{25}{2}$$

$$b = 1,\ q = 0 \quad : \quad d_A = \overline{d} \quad d_B = \underline{d} \quad \Pi_A^{AA} = \tfrac{22}{3} \quad \Pi_B^{AA} = 23$$

$$b = \tfrac{1}{2},\ q = \tfrac{1}{2} \quad : \quad d_A = \overline{d} \quad d_B = \underline{d} \quad \Pi_A^{AA} = \tfrac{49}{12} \quad \Pi_B^{AA} = \tfrac{25}{2}$$

$$b = 1,\ q = \tfrac{1}{2} \quad : \quad d_A = \overline{d} \quad d_B = \underline{d} \quad \Pi_A^{AA} = \tfrac{91}{12} \quad \Pi_B^{AA} = 23$$

$$b = \tfrac{1}{2},\ q = 1 \quad : \quad d_A = \overline{d} \quad d_B = \underline{d} \quad \Pi_A^{AA} = \tfrac{13}{3} \quad \Pi_B^{AA} = \tfrac{25}{2}$$

$$b = 1,\ q = 1 \quad : \quad d_A = \overline{d} \quad d_B = \underline{d} \quad \Pi_A^{AA} = \tfrac{47}{6} \quad \Pi_B^{AA} = 23$$

One can see that in a any of the examples firm A will choose $d_A = \overline{d}$, with firm B's response given by $d_B = \underline{d}$. This leaves both firms with positive profits.

Two-period model with $r > 0$

Scenario a): $0 > \Delta b(\underline{\theta}) > \Delta b(\overline{\theta})$

For both periods we get the same pricing functions as in the one-period model:

$$p_{B,t}^* = \frac{1}{2}(r + p_{A,t} + \mu(c(\overline{\theta}, d_A) - c(\overline{\theta}, d_B)) + (1 - \mu)(c(\underline{\theta}, d_A) - c(\underline{\theta}, d_B)) - q\alpha_B)$$

$$p_{A,t}^* = \frac{1}{2}(3r - \mu(c(\overline{\theta}, d_A) - c(\overline{\theta}, d_B)) - (1 - \mu)(c(\underline{\theta}, d_A) - c(\underline{\theta}, d_B)) - q\alpha_A - q\alpha_B)$$

Comparison of profits for the data requirement decisions also yields again:

$$d_j^* = \begin{cases} \underline{d} \text{ if } \mu\Delta c(\overline{\theta}) + (1 - \mu)\Delta c(\underline{\theta}) > q \\ \overline{d} \text{ otherwise} \end{cases}$$

Thus, we have two equilibria. If $\mu\Delta c(\overline{\theta}) + (1 - \mu)\Delta c(\underline{\theta}) > q$:

$$(d_A^* = \underline{d}, p_{A,t}^* = \frac{3r}{2}), (d_B^* = \underline{d}, p_{B,t}^* = \frac{5r}{4}), \forall t$$

and if $\mu\Delta c(\overline{\theta}) + (1 - \mu)\Delta c(\underline{\theta}) \le q$:

$$(d_A^* = \overline{d}, p_{A,t}^* = \frac{3r}{2} - q), (d_B^* = \overline{d}, p_{B,t}^* = \frac{5r}{4} - q), \forall t$$

Study on monetising privacy

An economic model for pricing personal information

The similarity to the one-period model is due to the fact that without personalisation the second period is just the repetition of the first periods pricing decision. As there is no lock in, there is no additional surplus to be distributed.

Scenario b): $\Delta b(\underline{\theta}) > 0 > \Delta b(\overline{\theta})$

Using the result from the one-period model that both firms choose the same data requirement, we focus on the case with $d_A = d_B = \underline{d}$. With $d_A = d_B = \overline{d}$ we would get the same results expect that equilibrium prices are reduced by q.

Solving the model with backward induction, we first have to analyse the firms' and consumers' behaviour in the second period. Taking into account that all types consumers may switch in the second period, we first show that there are no equilibria in which consumers with $\underline{\theta}$ do actually switch. We then characterise the equilibria where all consumers of type $\underline{\theta}$ opt for personalisation and do not switch in the second period.

Equilibrium with both types of consumers switching:

First we show that an equilibrium in which consumers with $\theta_i = \underline{\theta}$ switch firm does not exist.

We first consider the case in which consumers, who have bought from firm *A* in the first period, buy from firm *B* in the second period.

In order to do so we construct indifferent consumers for both types:

$$i_2^c(\underline{\theta}) = \frac{r - p_{A,2} + p_{B,2} + b}{2r}$$

$$i_1^c(\underline{\theta}) = \frac{r - p_{A,1} + p_{B,1} - b}{2r}$$

$$i_2^c(\overline{\theta}) = \frac{r - p_{A,2} + p_{B,2}}{2r}$$

$$i_1^c(\overline{\theta}) = \frac{r - p_{A,1} + p_{B,1}}{2r}$$

Note that $i_2^c(\underline{\theta})$ denotes an indifferent consumer of type $\underline{\theta}$, who is indifferent between buying from firm *A* in both periods and switching from *A* to *B*. This means $i_1^c(\underline{\theta})$ is thought of as being indifferent between switching from *A* to *B* and staying with *B* in both periods. For consumers of type $\overline{\theta}$, $i_t^c(\overline{\theta})$ denotes the indifferent consumer in period *t*.

To start with the firms' pricing decisions we use the part of the profit function, which relates to the second period. Thus, we get:

$$\Pi_{j,2} = n_{j,2} p_{j,2}$$

According to the indifference conditions above, we can rewrite the second period profit function as:

$$\Pi_{A,2} = ((1 - \mu)i_2^c(\underline{\theta}) + \mu i_2^c(\overline{\theta})) p_{A,2}$$

$$\Pi_{B,2} = ((1-\mu)(1-i_2^c(\underline{\theta})) + \mu(1-i_2^c(\overline{\theta})))p_{B,2}$$

For firm B we derive the optimal reaction function, by plugging in the indifferent consumers and differentiating the profit function with respect to price:

$$p_{B,2}^r = \frac{r-(1-\mu)b+p_{A,2}}{2}$$

By doing the same for firm A and plugging in B's reaction we derive:

$$p_{A,2}^* = \frac{3r+(1-\mu)b}{2}$$

Plugging back into the reaction function above we then derive:

$$p_{B,2}^* = \frac{5r-(1-\mu)b}{4}$$

For the second period indifferent consumers we thus get:

$$i_2^c(\underline{\theta}) = \frac{3r+b(1+3\mu)}{8r}$$

$$i_2^c(\overline{\theta}) = \frac{3(r-b(1-\mu))}{8r}$$

Now, let us turn to the first period. We now consider the following profit functions:

$$\Pi_{A,1} = ((1-\mu)i_1^c(\underline{\theta}) + \mu i_1^c(\overline{\theta}))p_{A,1} + \pi_{A,2}$$

$$\Pi_{B,1} = ((1-\mu)(1-i_1^c(\underline{\theta})) + \mu(1-i_1^c(\overline{\theta})))p_{B,1} + \pi_{B,2}$$

Again, we derive the reaction function for firm B:

$$p_{B,1}^r = \frac{r+(1-\mu)b+p_{A,1}}{2}$$

This leads to the optimal pricing for firm A and in turn also for firm B:

$$p_{A,1}^* = \frac{3r-(1-\mu)b}{2}$$

$$p_{B,1}^* = \frac{5r+(1-\mu)b}{4}$$

Then we again get the location of indifferent consumers in the first period:

$$i_1^c(\underline{\theta}) = \frac{3r-b(1+3\mu)}{8r}$$

$$i_1^c(\overline{\theta}) = \frac{3(r+b(1-\mu))}{8r}$$

By construction we would require $i_1^c(\underline{\theta}) > i_2^c(\underline{\theta})$. However, this does not hold here and thus optimal pricing decisions lead us to a contradiction.

For the case of consumers switching from firm B to firm A, we get the similar results, which are derived accordingly. For the second period we now get:

$$p_{A,2}^* = \frac{3r - (1-\mu)b}{2}$$

$$p_{B,2}^* = \frac{5r + (1-\mu)b}{4}$$

$$i_2^c(\underline{\theta}) = \frac{3r - b(1 + 3\mu)}{8r}$$

For the first period, the results are now:

$$p_{A,1}^* = \frac{3r + (1-\mu)b}{2}$$

$$p_{B,1}^* = \frac{5r - (1-\mu)b}{4}$$

$$i_1^c(\underline{\theta}) = \frac{3r + b(1 + 3\mu)}{8r}$$

Again, the necessary condition that $i_1^c(\underline{\theta}) < i_2^c(\underline{\theta})$ holds is violated.

Now, let us consider the possible corner solution, in which one firm sets a second period price, such that all consumers choose this firm. Therefore, assume any first period market share $n_{A,1}$ and any second period price $p_{A,2}$. If firm B wants to get all consumers in the second period, it has to choose a strategy $p_{B,2}^m = p_{A,2} - b - r$ in order to compensate the consumer for whom choosing B is least favourable. Note that firm A would make zero profits in this period. Therefore, it could just lower the price according to a standard undercutting- argument until profits are driven out of the market. In such a situation firm B could choose to sacrifice a few consumers, but making positive profits on all other consumers with a slight increase of $p_{B,2}$.

Thus, switching to another strategy as $p_{B,2}^m$ is beneficial for firm B and thus one would have to consider candidates for an interior solution again.[62]

But as these candidates have already been shown to lead to contradictions, we are able to conclude that this type of equilibrium does not exist in this game.

Equilibrium with only consumers with a high concern switching:

Turning to the equilibria where only consumers with $\bar{\theta}$ switch, we first characterise the firms' pricing strategies in the second period. We then turn to the first period decisions of the consumers and the firms.

---

[62] *A similar argument can be constructed for firm* A *as well.*

Study on monetising privacy

An economic model for pricing personal information

Calculating the firms' pricing decisions in the second period, we have to take into account that the firms' demand functions are kinked. More precisely, while the indifferent consumer $i_2^c(\overline{\theta})$ is given by

$$i_2^c(\overline{\theta}) = \min\left\{1, \max\left\{0, \frac{p_{B,2} - p_{A,2} + r}{2r}\right\}\right\}$$

firms also have the option to set their prices such that consumers with $\underline{\theta}$ would switch. Note that although this pricing strategy cannot be part of an equilibrium we nevertheless have to specify the induced profits as we have to calculate all deviation profits in the second period. Using $\Delta b(\underline{\theta}) > 0$ and assuming that all consumers with $\underline{\theta}$ opted for personalisation, the indifferent consumer $i_2^c(\underline{\theta})$ is given by

$$i_2^c(\underline{\theta}) = \begin{cases} \underline{i}_2^c(\underline{\theta}) := \max\{0, \frac{p_{B,2} - p_{A,2} + r + b}{2r}\} & \text{if} \quad p_{B,2} - p_{A,2} \leq -b - r(1 - 2i^c(\underline{\theta})) \\ i^c(\underline{\theta}) & \text{if} \quad -b - r(1 - 2i^c(\underline{\theta})) \leq p_{B,2} - p_{A,2} \leq b - r(1 - 2i^c(\underline{\theta})) \\ \overline{i}_2^c(\underline{\theta}) := \min\{\frac{p_{B,2} - p_{A,2} + r - b}{2r}, 1\} & \text{if} \quad p_{B,2} - p_{A,2} \geq b - r(1 - 2i^c(\underline{\theta})) \end{cases}$$

where $i^c(\underline{\theta})$ denotes the consumer with $\underline{\theta}$ who was indifferent between buying from firm A and firm B in the first period.

Using $i_2^c(\overline{\theta})$ and $i^c(\underline{\theta})$ the firms' profits in the second period can be written as

$$\Pi_{A,2} = \begin{cases} \Pi_{A,2}^1 = p_{A,2}\left[\mu\, i_2^c(\overline{\theta}) + (1 - \mu)\, \underline{i}_2^c(\underline{\theta})\right] & \text{if} \quad p_{B,2} - p_{A,2} \leq -b - r(1 - 2i^c(\underline{\theta})) \\ \Pi_{A,2}^2 = p_{A,2}\left[\mu\, i_2^c(\overline{\theta}) + (1 - \mu)\, i^c(\underline{\theta})\right] & \text{if} \quad -b - r(1 - 2i^c(\underline{\theta})) \leq p_{B,2} - p_{A,2} \leq b - r(1 - 2i^c(\underline{\theta})) \\ \Pi_{A,2}^3 = p_{A,2}\left[\mu\, i_2^c(\overline{\theta}) + (1 - \mu)\, \overline{i}_2^c(\underline{\theta})\right] & \text{if} \quad p_{B,2} - p_{A,2} \geq b - r(1 - 2i^c(\underline{\theta})) \end{cases}$$

as well as

$$\Pi_{B,2} = \begin{cases} \Pi_{B,2}^1 = p_{B,2}\left[\mu(1 - i_2^c(\overline{\theta})) + (1 - \mu)(1 - \underline{i}_2^c(\underline{\theta}))\right] & \text{if} \quad p_{B,2} - p_{A,2} \leq -b - r(1 - 2i^c(\underline{\theta})) \\ \Pi_{B,2}^2 = p_{B,2}\left[\mu(1 - i_2^c(\overline{\theta})) + (1 - \mu)(1 - i^c(\underline{\theta}))\right] & \text{if} \quad -b - r(1 - 2i^c(\underline{\theta})) \leq p_{B,2} - p_{A,2} \leq b - r(1 - 2i^c(\underline{\theta})) \\ \Pi_{B,2}^3 = p_{B,2}\left[\mu(1 - i_2^c(\overline{\theta})) + (1 - \mu)(1 - \overline{i}_2^c(\underline{\theta}))\right] & \text{if} \quad p_{B,2} - p_{A,2} \geq b - r(1 - 2i^c(\underline{\theta})) \end{cases}$$

We are now maximising $\Pi_{B,2}$ with respect to $p_{B,2}$ and let $p_{B,2}^*$ denote the optimal price for firm B, i.e. $p_{B,2}^* := \arg\max \Pi_{B,2}$ and note that $p_{B,2}^*$ - depending on the parameter constellations- is given by one of the following prices

$$p_{B,2}^1 := \arg\max \Pi_{B,2}^1 = \frac{1}{2}(p_{A,2} + r - (1 - \mu)b)$$

$$p_{B,2}^2 := \arg\max \Pi_{B,2}^2 = \frac{1}{2}(p_{A,2} - r(1 - 2i^c(\underline{\theta})) + \frac{1}{\mu}r(1 - i^c(\underline{\theta}))$$

$$p_{B,2}^{2c} := p_{A,2} + b - r(1 - 2i^c(\underline{\theta}))$$

$$p_{B,2}^3 := \arg\max \Pi_{B,2}^3 = \frac{1}{2}(p_{A,2} + r + (1\mu)b)$$

where $p_{B,2}^{2c}$ is the highest price $p_{B,2}$ such that no consumer with $\bar{\theta}$ switches. Using $p_{B,2}^*$ and turning to firm A, firm A's profit function can be written as

$$\Pi_{A,2} = \begin{cases} \Pi_{A,2}^{1*} = -\frac{1}{4r}\, p_{A,2}\big[p_{A,2} - (1-\mu)b - 3r\big] & \text{if} \quad p_{B,2}^* = p_{B,2}^1 \\ \Pi_{A,2}^{2*} = -\frac{1}{4r}\, p_{A,2}\big[\mu(p_{A,2} - r(2 - i^c(\underline{\theta})) - 2r(1 + i^c(\underline{\theta}))\big] & \text{if} \quad p_{B,2}^* = p_{B,2}^2 \\ \Pi_{A,2}^{2c} = \frac{1}{2r}\, b\mu p_{A,2} + p_{A,2} i^c(\underline{\theta}) & \text{if} \quad p_{B,2}^* = p_{B,2}^{2c} \\ \Pi_{A,2}^{3*} = -\frac{1}{4r}\, p_{A,2}\big[p_{A,2} + (1-\mu)b - 3r\big] & \text{if} \quad p_{B,2}^* = p_{B,2}^3 \end{cases}$$

Note for later reference, that $\Pi_{A,2}$ is linearly increasing in $p_{A,2}$ as long as $p_{B;2}^* = p_{B,2}^{2c}$. Furthermore, undercutting firm A and inducing some consumers with $\underline{\theta}$ to switch by choosing $p_{B,2}^* = p_{B,2}^1$ becomes more attractive for firm B the higher the price of firm A. Analysing $\Pi_{A,2}$ and calculating the optimal price $p_{A,2}^*$ for firm A we get the following set of possible equilibrium prices

$$p_{A,2}^* \in \big\{p_{A,2}^1, p_{A,2}^2, p_{A,2}^3, p_{A,2}^{c1}, p_{A,2}^{c2}\big\} \text{ with}$$

$$p_{A,2}^j := \arg \max \Pi_{A,2}^{i*} \text{ with } j = 1, 2, 3 \text{ and}$$

$$p_{A,2}^{c1} \text{ such that } \Pi_{B,2}^1 = \Pi_{B,2}^2 \text{ for } p_{B,2}^* = p_{B,2}^2 \text{ as well as}$$

$$p_{A,2}^{c2} \text{ such that } \Pi_{B,2}^1 = \Pi_{B,2}^2 \text{ for } p_{B,2}^* = p_{B,2}^{2c}$$

Taking into account that we are looking for an equilibrium in which consumers with $\underline{\theta}$ do not switch, we can focus on $p_{A,2}^2$ and $p_{A,2}^{c1}$ as well as $p_{A,2}^{c2}$ which are given by

$$p_{A,2}^2 = \frac{r}{2\mu}\big[2 + \mu + 2i^c(\underline{\theta})(1-\mu)\big]$$

$$p_{A,2}^{c1} = b + r + \frac{1}{\sqrt{\mu}}\big[b\mu + 2r(1 - i^c(\underline{\theta}))\big] - 2r\, i^c(\underline{\theta})$$

$$p_{A,2}^{c2} = b - 3b\mu + 2\sqrt{2}\sqrt{b(1-\mu)(2r(1 - i^c(\underline{\theta})) - b\mu)} + r(3 - 4i^c(\underline{\theta}))$$

Turning to the first period, we start with the decisions of the consumers. While the indifferent consumer with $\bar{\theta}$ is again given by

$$i_1^c(\bar{\theta}) = \min\{\max\{0, \frac{p_{B,1} - p_{A,1} + r}{2r}\}, 1\}$$

the indifferent consumer with $\underline{\theta}$, i.e. $i^c(\underline{\theta})$, is implicitly given by the solution of the following equation (assuming interior solutions)

$$b - p_{A,1} - p_{A,2}^* - 2r\, i^c(\underline{\theta}) = b - p_{B,1} - p_{B,2}^* - 2r\,(1 - i^c(\underline{\theta}))$$

where the second period equilibrium prices $p_{A,2}^*$ and $p_{B,2}^*$ are functions of $i^c(\underline{\theta})$ (see above). Solving this equation for the candidate equilibrium prices we get, assuming again $i^c(\underline{\theta}) \in (0,1)$

Study on monetising privacy

An economic model for pricing personal information

enisa
European Network
and Information
Security Agency

69

$$p_{A,2}^* = p_{A,2}^2 \text{ and } p_{B,2}^* = p_{B,2}^2 \rightarrow i^c(\underline{\theta}) = \frac{1}{2r(3+5\mu)}\left[2r + \mu(4(p_{B,1}-p_{A,1})+5r)\right]$$

$$p_{A,2}^* = p_{A,2}^{c1} \text{ and } p_{B,2}^* = p_{B,2}^2 \rightarrow i^c(\underline{\theta}) = \frac{1}{2r(1-\sqrt{\mu}+2\mu)}\left[2(r - r\sqrt{\mu} + \mu(p_{B,1}-p_{A,1}+r)) - b(\mu + \mu^{3/2})\right]$$

$$p_{A,2}^* = p_{A,2}^{c2} \text{ and } p_{B,2}^* = p_{B,2}^{2c} \rightarrow i^c(\underline{\theta}) = \frac{1}{2r}\left[b + r + p_{B,1} - p_{A,1}\right]$$

Given the second period profits as well as $i^c(\underline{\theta})$, we are now able to specify the firms' overall profits:

$$\Pi_A = p_{A,1}\left[\mu\, i_1^c(\overline{\theta}) + (1-\mu)i^c(\underline{\theta})\right] + \Pi_{A,2}\Big|_{P_{A,2}=p_{A,2}^*,\, P_{B,2}=p_{B,2}^*}$$

$$\Pi_B = p_{B,1}\left[\mu(1 - i_1^c(\overline{\theta})) + (1-\mu)(1 - i^c(\underline{\theta}))\right] + \Pi_{B,2}\Big|_{P_{A,2}=p_{A,2}^*,\, P_{B,2}=p_{B,2}^*}$$

Using these profit functions and calculating the firms' optimal prices reveals that the equilibrium prices are given by $p_{A,2}^* = p_{A,2}^2$ and $p_{B,2}^* = p_{B,2}^2$ as long as μ is high enough. To be more specific, using the same parameter constellations as in the case with zero transportation costs and calculating the firms' profits for all possible deviations, shows that $\mu \geq 1/4$ suffices to guarantee that the firms' pricing decisions in the first period lead to an interior equilibrium with $p_{A,2}^* = p_{A,2}^2$ and $p_{B,2}^* = p_{B,2}^2$ in the second period. Solving for the optimal first period prices $p_{A,1}^*$ and $p_{B,1}^*$, we get that the firms' reduced profit functions do not depend on q and b. More precisely, we obtain

$$\Pi_A^* = p_{A,1}^*\left[\mu\, i_1^c(\overline{\theta}) + (1-\mu)i^c(\underline{\theta})\right] + \Pi_{A,2}\Big|_{P_{A,2}=p_{A,2}^*,\, P_{B,2}=p_{B,2}^*}$$

$$= \frac{(473 + \mu(1834 + \mu(1937 + 4\mu(87 + 4\mu))))}{\mu(7+\mu)^2(19 + 3\mu(14+\mu))}r$$

$$\Pi_B^* = p_{B,1}^*\left[\mu(1 - i_1^c(\overline{\theta})) + (1-\mu)(1 - i^c(\underline{\theta}))\right] + \Pi_{B,2}\Big|_{P_{A,2}=p_{A,2}^*,\, P_{B,2}=p_{B,2}^*}$$

$$= \frac{2(8901 + \mu(47424 + \mu(83307 + \mu(53252 + \mu(10999 + \mu(892 + 25\mu))))))}{\mu(7+\mu)^2(19 + 3\mu(14+\mu))^2}r$$

Differentiating Π_A^* and Π_B^* with respect to μ reveals that both profits are decreasing in μ. Intuitively, the higher μ, the lower is the fraction of consumers who choose personalisation and thus the lower the fraction of consumers who are locked-in in the second period. Since second period equilibrium prices decrease in μ, an increase in μ reduces the firms' profits. Considering first period decisions, firm B can anticipate that the price firm A will choose in the second period is the higher the more personalising consumers firm A has attracted in the first period. Firm B's incentive to increase its first period demand by choosing a rather low price is therefore higher for an increased μ, i.e the lower the number of consumers who opt for personalisation. Taking these effects together, shows that equilibrium prices in both periods and thus the firms' profits decrease with μ.

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu

Exhibit P

J O I N T   C E N T E R
AEI-BROOKINGS JOINT CENTER FOR REGULATORY STUDIES

The Value of Online Information Privacy:
An Empirical Investigation

Il-Horn Hann, Kai-Lung Hui, Tom S. Lee, and I.P.L. Png

Related Publication 03-25
October 2003

Executive Summary

Concern over online information privacy is widespread and rising. However, prior research is silent about the value of information privacy in the presence of potential benefits from sharing personally identifiable information. Analyzing individuals' trade-offs between the benefits and costs of providing personal information to websites revealed that benefits – monetary reward and future convenience – significantly affect individuals' preferences over websites with differing privacy policies. Quantifying the value of website privacy protection revealed that among U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – 44.62. Finally, three distinct segments of Internet consumers were determined – privacy guardians, information sellers, and convenience seekers.

1

The Value of Online Information Privacy: An Empirical Investigation
Il-Horn Hann, Kai-Lung Hui, Tom S. Lee, and I.P.L. Png

1. Introduction

Privacy has been identified to be a major, if not the most critical, impediment to e-commerce: "In our view, the single, overwhelming barrier to rapid growth of e-commerce is a lack of consumer trust that consumer protection and privacy laws will apply in cyberspace. Consumers … worry, deservedly, that supposedly legitimate companies will take advantage of them by invading their privacy to capture information about them for marketing and other secondary purposes without their informed consent" (U.S. Public Interest Research Group 2000).

Even before the advent of e-commerce, there was broad concern about collection of personal information in various contexts, including employment, retailing and direct marketing, and government. These concerns prompted government action. In 1974, the U.S. Congress passed the Privacy Act to regulate government collection and use of personal information.[1] In 1980, the Organization for Economic Co-operation and Development published guidelines for the collection and use of personal information by government and private organizations (OECD 1980). Further, in 1995, the European Union adopted a data protection directive that regulates information within and beyond the Union (European Union 1995). The directive disallows transfer of information to other countries that do not provide adequate protection.

Rapid improvements in computing technologies and the advent of e-commerce have amplified public concern about privacy, especially on electronic networks. With every website visit, a browser leaves an electronic trace which can later be retrieved and analyzed. Combined with technology to store identifying information (cookies), website operators can profile browsers to an unprecedented degree and subsequently merge these profiles with other demographic data. Such an enriched data set can then be used by the company or sold to other parties.[2] This information could benefit the customer by more precisely identifying her need. However, it could also be used to her detriment. For example, Amazon.com was suspected of engaging in differential pricing based on prior shopping information and other customer

---

[1] Specifically, the Privacy Act of 1974 prohibits unauthorized disclosures of records and gives individuals the right to review records about themselves to check whether records have been disclosed and to request corrections or amendments.
[2] New York Times, "Giving the Web a Memory Cost Its Users Privacy," September 4, 2001.

2

demographics for the sales of DVDs.[3]   Westin (2001) concludes: "There has been a well-documented transformation in consumer privacy attitudes over the past decade, moving concerns from a modest matter for a minority of consumers in the 1980s to an issue of high intensity expressed by more than three-fourth of American consumers in 2001".

Despite the passage of new legislation, including the 1998 Children's Online Privacy Protection Act, which regulates the online collection and use of children's personal information, there continues to be public pressure for increased regulation. Over fifty bills to regulate online privacy were introduced in the first session of the 107th Congress. Industry, however, is resisting the proposals to tighten regulation. The national cost of complying with these legislative proposals has been estimated to be US$9-36 billion (Hahn 2001). For just catalog and Internet clothing retailers, a study sponsored by the Direct Marketing Association estimated that opt-in restrictions to use of demographic information by third parties would raise costs by US$1 billion (Turner 2001).

The conflict between privacy advocates and industry motivates our research objective: Exactly how much do individuals perceive to be the cost of releasing personal information online? The real policy issue is not whether consumers value online privacy. It is obvious that people value online privacy. What is not known is how much people value online privacy and the extent to which people differ in their valuations. Despite tremendous debate and policy interest, there has, to date, been no research into this question (Hahn 2001). Indeed, it has been conjectured that "measuring the value of consumer privacy may prove to be intractable" (Ward 2001).

Businesses need to know the value of privacy in deciding whether to invest in privacy seals and what incentives to offer consumers for their personal information. Governments need this information to decide on public policy towards information privacy. For instance, Laudon (1996) and Varian (1997) have proposed to regulate privacy through markets in personal information. But the economic viability of such markets depends on individuals' perceived value of privacy.

In this study, we applied conjoint analysis, which is the standard way of measuring consumer trade-offs (Green and Srinivasan 1990; Wittink and Cattin 1989), to U.S. and

---

[3] Amazon has subsequently apologized for charging different prices and refunded an average of $3.10 to each of 6,896 customers who bought a DVD. These consumers paid between 25-66 percent more than the lowest available price. While it has been

3

Singapore subjects' rankings of alternative combinations of benefits and privacy protection in an online setting. The benefits were monetary reward and future convenience, while the privacy protection applies to errors in storing or processing personal information, unauthorized secondary use of information, and improper access to information.[4] This allows us to make the following contributions:

First, the conjoint analysis showed that the benefits had a significant effect on our subjects' preferences. Second, by comparing the value of protection on the three privacy concerns with the value of monetary reward, we provide the first estimates of the monetary value of privacy protection in the United States. Last, by applying cluster analysis to the subjects' marginal rankings of the various benefits and concerns, we found that our subjects could be categorized into three distinct segments – privacy guardians, information sellers, and convenience seekers. The majority of subjects were relatively sensitive to online information privacy concerns ("privacy guardians"). By contrast, a smaller proportion was relatively willing to provide information in exchange for money ("information sellers"), and an even smaller proportion was relatively willing to provide information in exchange for convenience ("convenience seekers").

All of the preceding results were robust in the sense that they held in both the U.S. and Singapore samples. Our results contribute directly to the public policy debate over whether online privacy protection is worth its cost to industry. They also inform businesses whether to invest in privacy seals and what incentives to offer consumers for their personal information.

The remainder of this paper is organized as follows. We provide an overview of the relevant literature and our research questions in Section 2. The experimental procedure is explained in Section 3. Section 4 describes the results of the conjoint analysis and estimates the dollar value of privacy protection. Section 5 reports the results of the cluster analysis. Section 6 discusses implications for public policy and business strategy. Section 7 concludes with limitations and directions for future research.

---

speculated that Amazon engaged in price discrimination, Amazon claimed that these were 'random' tests. (http://www.internetnews.com/ec-news/article.php/4_471541, September 28, 2000).

4

2. <u>Theory and Hypotheses</u>

Information privacy has been defined as the individual's ability to control the collection and use of personal information (Westin 1967; Stone and Stone 1990). Research in consumer psychology suggests that individuals seek privacy to maintain self-identity, establish personal boundaries, and avoid unwanted disclosure and intrusion (Goodwin 1991, 1992). In many experimental and organizational settings, people are found to perceive privacy invasions when they are not granted sufficient control on the solicitation, storage, use and disclosure of various types of personal information (see, e.g., Eddy et al. 1999; Tolchinsky et al. 1981; Woodman et al. 1982). Such perception may deter them from taking part in transactions that involve personal information solicitation (Culnan 1993; Stone et al. 1983).

Consumer research suggests that individuals face a degree of risk when they enter into marketing transactions, and their perceived risk may significantly affect their extent of information search and purchase decisions (Cox and Rich 1964). Generally, perceived risk encompasses both the uncertainty and adverse consequences of taking part in a transaction (Dowling and Staelin 1994). Advances in network and telecommunications technologies have fostered the growth of electronic commerce, which has added a new information dimension to marketing transactions. Increasingly, consumer information is acquired, exchanged, and used by online merchants. This has expanded the risk of consumers – other than the basic products (or services), they now face an additional uncertainty regarding how their personal information is handled. Information privacy has been found to be of utmost concern to consumers in contemporary marketing exchanges (Culnan and Armstrong 1999; Hoffman et al. 1999; Phelps et al. 2000).

One perspective through which the information privacy context of an Internet relationship between a consumer and a firm can be discussed is Social Exchange Theory (SET). In its most general form, social exchange theory proposes that people review and weigh their relationships in terms of costs and rewards. These costs and rewards are specific to a person and are used to guide behavior (Thibaut and Kelley 1959; Homans 1961; Blau 1964). This notion has found widespread application in diverse areas; social exchange theory has been used to understand marketing transactions (Alderson and Martin 1965; Bagozzi 1975), to predict the

---

[4] The objective of this research certainly fits within Wittink's (2001) "Encapsulation Model" in which business school research

perception of service level obtained from a government agency (Gutek 1999) and to analyze the reciprocity of venture capitalists to invite other venture capitalists to join in a continued funding of a start-up (Jan Piskorski). Specifically, in the context of online marketing, Chellappa and Sin (2002) propose several hypotheses based on social exchange theory.

Invoking social exchange theory to analyze the Internet relationship, we first have to establish the costs and rewards to submitting private information to a firm. Regarding the costs, we identified the four concern dimensions previously established by Smith et al. (1996) – collection, error, unauthorized secondary use, and improper access. Collection refers to the concern that "extensive amounts of personally identifiable data are being collected and stored in databases"; error refers to the concern that "protections against deliberate and accidental errors in personal data are inadequate"; unauthorized secondary use refers to the concern that "information is collected for one purpose but is used for another, secondary purpose"; improper access refers to the concern that "data about individuals are readily available to people not properly authorized to view or work with this data" (Smith et al. 1996, page 172, Table 2). These dimensions were further validated by Stewart and Segars (2002).

In online transactions, firms seek to reduce these costs through notices and protections which are often provided in the form of a detailed privacy statement. Because of the extra risk associated with the use of personal information, consumers value informed notices of how their information is handled, and they prefer fair information procedures and privacy protection (Culnan and Armstrong 1999; Hoffman et al. 1999). Hence social exchange theory would suggest that consumers prefer websites that reduce these costs. In addition, the expectancy theory-based model of privacy suggests that individuals seek to minimize negatively valued outcomes, which include physical and psychological harms due to the misuse of personal information. Further, individuals' cognition of the desirability of the expected outcome due to disclosure is a direct, positive function of procedural factors related to information handling (Stone and Stone 1990). Therefore, our first hypothesis is formulated as:

> **Hypothesis H1**: Individuals value information privacy protection in online transactions that involve personal information solicitation; a website that provides a higher level of protection will be preferred to one that provides less protection.

---

must have real-world relevance.

Besides information privacy protection, individuals' preference toward a particular website may also be affected by extrinsic, positive reinforcements. The resource exchange theory characterizes six categories of interpersonal resources: love, status, information, money, goods and services, and it is well demonstrated that people are willing to trade one resource for another (Foa 1971; Donnenwerth and Foa 1974). Prior research has shown that this resource framework is quite general, and it can be applied to analyze different types of marketing transactions that involve interpersonal relationships and resource exchanges (Brinberg and Wood 1983; Hirschman 1987).

On the Internet, many websites provide monetary reward or exclusive, convenient services that help reduce transaction time to consumers who disclose certain personal information.[5] Both money and service are primary elements in Foa's (1971) theory, and they may act as positive incentives and resources for online firms to exchange for consumer information. Further, because privacy protection represents another type of service provided by online firms, the resource exchange theory predicts that people may be willing to forgo privacy protection in return for other resources (i.e., money or convenient services). Indeed, anecdotal evidence has shown that people are willing to disclose personal information for gifts and catalogs (Oberndorf 1999; Russell 1989), and even a $100 drawing (Jupiter Media Metrix 2002). The human capital model in economics also treats time as a primary resource to produce household activities (Becker 1965; Leclerc et al. 1995; Ratchford 2001). This implies that people may value services provided by websites that increase convenience and help save time, which can then be used for other consumption activities.

The proposition that individuals value positive reinforcements when deciding whether to provide information to websites is also consistent with social exchange theories. Specifically, the social exchange framework of human behavior posits that people tend to perform actions that generate outcomes which, based on their past experience and personal interest, are rewarding to them (Blau 1964; Emerson 1972a, 1972b; Homans 1961). The more rewarding is a particular outcome, the higher the probability that people will perform the associated action.

Because money and convenient service are both useful resources that most people find rewarding (Foa 1971), the social exchange theory suggests that people have a higher tendency to

---

[5] For instance, it is common for websites to offer shopping vouchers or discount coupons to first-time consumers who register as members; Amazon's one-click shopping facilitates quicker and easier transactions for customers who have previously provided personal information, such as delivery address and credit card profile.

enter into an exchange relationship with websites which provide more monetary reward or time-saving convenient services. Synthesizing the above theoretical arguments, our next hypotheses are posited as:

> **Hypothesis H2a**: Individuals value positive reinforcements, exemplified by *monetary reward*, in online transactions that involve personal information solicitation; a website that provides *higher levels of money* will be preferred to one that provides less money.

> **Hypothesis H2b**: Individuals value positive reinforcements, exemplified by *time-saving services*, in online transactions that involve personal information solicitation; a website that provides *higher levels of time-saving services* will be preferred to one that provides less time-saving.

Note that H1, H2a and H2b describe basic individual preferences, and they may apply to general behavioral decisions, such as participation into online activities, information disclosure, or selection of websites for transactions. In particular, when individuals are presented with multiple websites that differ in terms of privacy protection or the provision of positive reinforcements, they may tradeoff the value that they attach to each of these dimensions.

Theoretical models of privacy have suggested that individuals perform a privacy calculus to assess the cost and benefit of providing personal information (Laufer and Wolfe 1977; Stone and Stone 1990). In the online context, privacy cost consists of consumers' perceived risk of information provision (cf. H1), whereas benefit can be any monetary rewards or services that consumers receive from websites (cf. H2a, H2b). Such a cost-benefit tradeoff calculus is coherent with Foa's (1971) resource exchange hypothesis, as consumers may forgo privacy protection (a service resource) to acquire more money or services. Empirically, research has found that people often make tradeoff decisions involving money and time (Leclerc et al. 1995). In the context of direct mail participation, Milne and Gordon (1993) exposed subjects to a trade-off between compensation, targeting, volume, and permission, thereby making perceptions about negative consequences of revealing private information implicit. In their study, monetary compensation received the highest weight. As we illustrate later, a conjoint experiment allows us to test H1, H2a and H2b, to explore the extent of such cost-benefit privacy tradeoff explicitly, and to quantify the monetary value of different privacy protections.

Finally, the social exchange theory posits that individuals' choice of actions (and hence their preferences toward alternative stimuli) are influenced by their personal experience; the more frequently a person was rewarded by a particular stimulus in the past, the more likely she

would be to perform an action that leads to the stimulus (Emerson 1972a; Homans 1961). Also, the extent of privacy calculus posited by Laufer and Wolfe (1977) depends on personal and environmental characteristics, and Stone and Stone's (1990) expectancy theory-driven privacy model includes individual and social factors such as personality and previous learning. In accordance with these models, individuals' preferences toward privacy protection and positive reinforcement may be shaped by their personal characteristics. In the context of information privacy, these theories posit that individuals may vary in their judgments towards online privacy. In as much as expectations about rewards and costs across individuals are similar, groups may be identified. For example, past opinion surveys have divided the U.S. population into a majority of "privacy pragmatists" and minorities of "privacy fundamentalists" and "privacy unconcerned" (Westin 2001). In this research, other than testing the hypotheses and assessing privacy tradeoff, we use a variety of personal characteristics as predictors to verify whether such a categorization is appropriate, and whether individuals' attitudes toward privacy can be systematically predicted.

3. Experimental Procedure

To address our primary set of research questions, we employed the technique of conjoint analysis. This technique presents test subjects with a set of alternatives (stimuli). Each stimulus consists of particular levels of various dimensions. The subject is asked to rank the stimuli according to her own preferences. Conjoint analysis assumes that the individual's ranking of each stimulus can be decomposed into the sum of contributions from the multiple dimensions. For each dimension, the contribution is the part-worth multiplied by the level of that dimension. Essentially, the part-worth is the marginal utility of the dimension in the individual's ranking of the conjoint stimuli.

To keep the conjoint tasks to a manageable size, Green and Srinivasan (1990) recommend that the number of attributes be limited to six or fewer. Following Green and Krieger (1991), we conducted focus groups prior to the conjoint study. Specifically, we conducted three focus group discussions with upper-division undergraduate and graduate students in the United States and Singapore to identify the key benefits that they expected from registration with websites and suitable attribute levels. The focus groups suggested that individuals clearly value direct monetary savings. In addition, they also identified convenience

as another important benefit of providing personal information to a website. The focus groups identified two sources of convenience benefits – the explicit time saving per session and the expected visit frequency to the website. Accordingly, we operationalized convenience by "expected visit frequency/total time savings" in our conjoint experiment.[6]

As mentioned before, we considered the four concern dimensions identified by Smith et al. (1996) – collection, error, unauthorized secondary use, and improper access – as the costs of privacy. For our purpose, collection is a necessary antecedent to the three other dimensions. Error, unauthorized secondary use and improper access of information can not happen without ex ante collection of personal information. Further, individuals' concerns on the other three dimensions are a direct function of the amount of information collected – the more information a website collects, the higher should be the concerns with error, unauthorized secondary use, and improper access of information. Therefore, it would not be appropriate to manipulate the collection of information and let subjects assess the tradeoffs between collection and other concern/benefit dimensions. Accordingly, in our conjoint analysis, we controlled for the collection of information and manipulated the other three concern dimensions.

Taken together, our conjoint study assessed trade-offs among five dimensions – two benefits and three privacy concerns. We created three treatment levels each of monetary reward ($5, $10 and $20) and visit frequency/time savings (monthly, weekly and daily).[7] The benefit levels were motivated by the focus groups. The three concerns (error, unauthorized secondary use and improper access of information) were manipulated by the presence (or absence) of proper information handling and access procedures.

Based on these five dimensions and their treatment levels, there were a maximum of 3 x 3 x 2 x 2 x 2 = 72 conjoint stimuli. To avoid asking subjects to rank too many alternatives, we selected 18 stimuli based on an optimal orthogonal design (Addelman 1962). For example, one particular stimulus was a website that provided a $5 monetary reward in return for personal information and which the subject visited once a month with a total time savings of 24 minutes per year. Further, the website had no error correction procedure, no policies to prevent

---

[6] The subjects were told during the experiments that if they expected to visit the website daily, their average time saving over the year would be 8 hours and 20 minutes (assuming an average saving of 2 minutes per transaction, 2 minutes x 5 days a week x 50 weeks = 8 hours and 20 minutes); if they expected to visit the website weekly, the yearly saving would be 1 hour and 40 minutes; and if they expected to visit the website monthly, the yearly saving would be 24 minutes.

[7] The monetary rewards were framed in the respective local currencies. As of April 2002, one Singapore dollar = 54 US cents. Due to the currency differences, the effective ranges of monetary rewards differed between the U.S. and Singapore experiments – in US dollars, the Singapore rewards were equivalent to US$2.70, US$5.40, and US$10.80, respectively.

unauthorized secondary use, and no policies to prevent improper access to information. Our conjoint analysis asked subjects to rank 18 websites (stimuli), which represented different combinations of benefits and privacy protection. In order to control for industry effects, we posed the conjoint stimuli in three settings – financial, healthcare, and travel. Within each of the three industries, we controlled for the degree of information collection by telling the subjects that all 18 stimuli (that is, hypothetical websites) requested the same set of personal information from the subjects. The personal information consisted of name, home address, phone number, e-mail address, credit card information, and some industry-specific information. In addition, travel websites requested the consumer's occupation, travel purpose, destination and frequency of travel, as well as frequent flyer numbers, healthcare websites asked for medical history, drug allergies, and prescription record, and financial websites asked for household income, stock portfolio, and previous stock trading experience.

Each subject was randomly assigned to one of the three industry settings and asked to rank the 18 stimuli (websites) according to her own preferences. In other words, the benefit/concern dimensions were within-subject factors whereas industry was a between-subject factor. To capture the background of the experimental subjects, we also included demographic questions regarding subjects' gender, age, Internet usage and previous experience with invasion of privacy.

To strengthen the external validity of our study, we conducted the conjoint experiment in both the USA and Singapore. The U.S. subjects were upper-division undergraduate students from a major Eastern university. The Singapore sample consisted of upper-division undergraduate students enrolled in an e-commerce technologies course at a major university. Table 1 presents some descriptive statistics about our subjects.

The experiment proceeded as follows. First, all subjects completed the demographic questions. Then, the experimental task and the meanings of the five dimensions were explained. Finally, the subjects ranked the 18 stimuli based on their personal preferences. In the U.S. sample, 84 participants completed the experiment, and, among them, 35 students received course credit, while the remainder were compensated with US$7.[8] In Singapore, 184 subjects completed the experiment and received course credit. We collected 268 responses in total.

11

4. Conjoint Analysis

The key outcome of conjoint analysis is the part-worths (marginal utilities) of the various dimensions that comprise the conjoint stimuli. To estimate the part-worths, we used least-squares regression with the subjects' rankings (from 1 to 18) as the dependent variable and indicators of the various levels of the two benefit and three privacy concern dimensions as the independent variables. Then, the coefficient of each independent variable would be the part-worth corresponding to that level of the dimension. Further, we calculated the relative importance of each dimension as the part-worth corresponding to the maximum level of that dimension divided by the sum of the part-worths corresponding to the maximum levels of all five dimensions. We expressed relative importance as a percentage.

Table 2 reports the means of the part-worths and relative importance for the U.S. and Singapore subjects. Note that the part-worths and relative importance for the U.S. and Singapore samples are not directly comparable as the monetary rewards were framed in the respective local currencies. At the April 2002 exchange rate, the rewards specified to the Singapore subjects were equivalent to US$2.70, US$5.40, and US$10.80 respectively.

We first examined whether the responses from the subjects differed across the three industries (financial, healthcare and travel). Since our U.S. and Singapore samples were relatively large, the central-limit theorem implies that the estimated part-worths for each independent variable should approximately follow a normal distribution. Based on this premise, we conducted one-way analysis of variance (ANOVA) and pairwise t-tests to compare the part-worths across the industries. The results suggested that the part-worths (or, equivalently, the subjects' preferences) were not statistically different across financial, healthcare and travel websites. Accordingly, in all subsequent analyses, we pooled the data across industries.

The part-worths on the privacy coefficients (error, improper access, unauthorized secondary use) show strong support for Hypothesis 1. A positive part-worth for a specific privacy dimension, which differs significantly from zero, indicates that subjects on average prefer a website with this privacy feature. For example, regarding the US sample, a privacy policy which restricts improper access will rise its ranking by 3.007 (out of 18). Referring to Table 2, the part-worths for protection against all three privacy concerns were statistically

---

[8] We found no statistically significant difference in part-worths between those who received course credit and those compensated

12

significant at the 1% level in both samples. Among U.S. subjects, the part-worth for review (which enabled an individual to correct errors in his/her personal information) was 2.968, while that for disallowing unauthorized secondary use was 2.118. Among Singapore subjects, the part-worths for error review and editing, restricting improper access, and disallowing unauthorized secondary use were 1.787, 3.374 and 4.604 respectively.

Comparing the part-worths between countries, we found that, consistent with previous research (Esrock and Ferre 1999; Milberg et al. 1995), Singapore subjects were relatively more concerned about improper access and unauthorized secondary use than errors in storing information. However, the U.S. subjects exhibited less concern for unauthorized secondary use than errors in storing information. Despite the discrepancy in relative preferences toward the different privacy protections across the two samples, our conjoint experiment confirmed previous findings that individuals are highly concerned about information privacy, and they value protective measures (Culnan and Armstrong 1999).

Our results indicate support for Hypothesis 2a; i.e., that positive reinforcements such as monetary rewards are valued. For the U.S. sample, the part-worth for a US$20 reward was 3.141 and was statistically significant. This means that a website offering a US$20 reward for personal information would raise its ranking by 3.141 (out of 18) as compared to an otherwise identical website offering the base level US$5 reward. Also, the part-worth for a US$10 reward was 1.327 and significant. For the Singapore sample, the part-worth for a S$20 reward was 1.388 and was statistically significant.   At the prevailing exchange rate, S$20 was equivalent to US$10.80, hence it was not surprising that the part-worth was much less than the US$20 part-worth in the U.S. sample (3.141). Interestingly, the S$20 part-worth among Singapore subjects (1.388) was very close to the US$10 part-worth among U.S. subjects (1.327). This result arose even though the base-level rewards were different in the two samples (S$5 and US$5 respectively). The part-worth for a S$10 reward in the Singapore sample was 0.232 but not statistically significant. Apparently, the subjects were willing to trade away privacy protection or convenience only when the monetary reward exceeded a threshold, which lay between S$10-20 (US$5.40 – 10.80).

Taken together, the results from the U.S. and Singapore samples suggest that a sufficiently large monetary reward did significantly increase the relative attractiveness of a

---

with US$7. Hence, we pooled both groups into a single sample.

website independent of its privacy policy. Further, when the monetary reward was relatively low (as in the Singapore sample), the marginal utility of the reward was increasing, and when the monetary reward was relatively high (as in the U.S. sample), the marginal utility tended to decrease. These results indicate that the attractiveness of a monetary reward relative to privacy protection or convenience might follow the "S"-shape as shown in Figure 1. The results are consistent with economic analysis that utility functions tend to be non-concave (Friedman and Savage 1948; Hartley and Farrell 2002).

We also find a support for Hypothesis 2b; i.e., that positive reinforcements such as time saving services, operationalized by visit frequency/time savings, are valued. Referring to Table 2, in the U.S. sample, the part-worth for weekly visit was significant at the 5% level, but the part-worth for daily visit was significant only at the 10% level. Further, the part-worths for weekly and daily visits were not significantly different. In the Singapore sample, the part-worths for visit frequency/time savings were generally more significant. However, as with the U.S. subjects, the effect due to weekly visit was not significantly different from that due to daily visit.

From the results of both samples, we conclude that there is some evidence that subjects are sensitive to convenience. The evidence is stronger among Singapore subjects than U.S. subjects. Further, once the subjects expected to visit a certain website sufficiently frequently (at least once a week), more frequent visits did not seem to affect the subjects' preferences.

The part-worths and relative importance associated with visit frequency/time savings among U.S. and Singapore subjects were very close. In both samples, these were much lower than the part-worths and relative importance for the other dimensions. Apparently, among our subjects, convenience was only a minor factor when evaluating websites. By contrast, monetary reward and privacy protection were perceived to be much more important.

We can use these results to calculate the marginal utility of a one-dollar reward. Referring to Table 2, in the U.S. sample, between the US$5 and US$10 rewards, the US$5 increase raised the ranking by 1.327, or 0.265 per dollar of reward. Alternatively, between the US$10 and US$20 rewards, the US$10 increase raised the ranking by 3.141 – 1.327 = 1.814, or 0.181 per dollar of reward. These two estimates provide a range of 0.181 – 0.265 per U.S. dollar of reward.[9] In the Singapore sample, the S$10 part-worth was not significantly different from zero. Accordingly, we focus on the S$20 part-worth. Between the S$5 and S$20 rewards, the

14

S$15 increase raised the ranking by 1.388, which amounted to 0.0925 per (Singapore) dollar of reward or 0.171 per U.S. dollar of reward. This was quite remarkably close to the range (0.181 – 0.265 per U.S. dollar of reward) that we found among U.S. subjects.

Finally, using the marginal utilities of a dollar reward and the part-worths for privacy protection, we estimate the value of protection, on a per-subject basis, for each of the three privacy concerns. Recall that we estimated the marginal utility of a US$1 reward to be 0.181 – 0.265 among the U.S. subjects. By Table 2, the part-worth for review and editing of information was 2.968. Using the lower bound for the marginal utility (0.181 per dollar), the value of review and editing of information is 2.968/0.181 = US$16.40. Using the upper bound for the marginal utility (0.265 per dollar), the value is 2.968/0.265 = $11.20. We can use the same method to derive the values of protecting against improper access and unauthorized secondary use. The results are reported in Table 3. We also computed the values for the Singapore subjects using the marginal utility of 0.171 per U.S. dollar.

Generally, our results in Table 3 suggest that websites might need to offer substantial monetary incentives to overcome individuals' concerns about error, improper access, and unauthorized secondary use of information. Among U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – 44.62.

5. Cluster Analysis

To address our secondary set of research questions – whether individuals systematically differ in their trade-off between benefits of disclosing personal information and privacy concerns, we applied cluster analysis (Green and Krieger 1991; Vriens et al. 1996). This technique groups subjects into distinct segments according to the similarity of their estimated part-worths for the various dimensions. In the present case, we apply cluster analysis to segment the subjects according to their estimated part-worths over the various benefits and dimensions of privacy protection.[10]

Specifically, we applied hierarchical cluster analysis using average between-group linkage with (dis)similarity measured by the squared Euclidean distance to both the U.S. and

---

[9] Between the US$20 and US$5 rewards, the US$15 increase raised the ranking by 3.141, or 0.210 per dollar of reward, which is within the range of 0.181 – 0.265 calculated using the other reward differences.

Singapore samples.   The hierarchical method was preferred because we had no a priori information on the number of clusters and initial cluster seeds/centers (Hair et al. 1998, pp. 493 - 498).   We used a distance measure for (dis)similarity as all the part-worths (the inputs to the cluster analyses) were derived from a common scale, the website rankings.

For each sample, we began the analysis with every subject constituting a separate cluster. We then examined the percentage drops in the similarity coefficient as clusters were progressively merged.   In both the U.S. and Singapore samples, we stopped at three clusters as further combination of any two clusters resulted in a sharp drop in similarity, a stopping rule recommended by Hair et al. (1998, pp. 499).   Table 4 reports the three clusters and the respective mean part-worths.   A small number of subjects could not be classified into any of the three clusters.   We excluded these observations from subsequent analysis and discussion.[11]

Consistent across the two samples, the majority of the subjects formed a cluster that could be characterized by a high value on information privacy.   Specifically, 72% of the U.S. subjects and 84% of the Singapore subjects exhibited relatively high part-worths for protection against error, improper access, and unauthorized secondary use of their personal information.   By contrast, their part-worths on monetary reward and visit frequency/time savings were relatively low.   We label this group of subjects as "privacy guardians" – people who attach a relatively high value to information privacy.

The next largest cluster consisted of subjects who attached a relatively high value to monetary reward.   We call them "information sellers", as they tend to "sell" personal information with little regard for convenience (visit frequency/time savings) or website privacy policies.

The smallest cluster comprised subjects who focused exclusively on convenience (operationalized by visit frequency/time savings).   In fact, their part-worths for visit frequency/time savings were so high that their preferences over alternative websites could almost be predicted by visit frequency/time savings alone.   We call these subjects "convenience seekers" – people who prefer convenience with little regard for money or website privacy policies.

---

[10] In the case of monetary reward and visit frequency/time savings, we used the maximum part-worths – $20 monetary reward and daily frequency respectively.

[11] Some of these outliers formed small (one- or two-member) clusters that we could not interpret. Several subjects exhibited unusual preferences such as preferring improper access to personal information. They possibly misunderstood the experimental tasks. The outliers constituted 7% and 10% of the U.S. and Singapore samples respectively.

16

Across the three clusters, we observe very different attitudes toward benefits and privacy. The privacy guardians prefer protection, but they still value monetary reward (the mean part-worth for monetary reward was significantly different from zero). Only the convenience seekers value convenience; for all other clusters, the part-worths for visit frequency/time savings were insignificant.[12]   Among the three privacy concerns, only unauthorized secondary use was significant in all three clusters.

Based on opinion surveys, Westin (2001, pp. 16) characterized 12% of the U.S. population as being "privacy unconcerned": "for 5 cents off, they will give you any information you want about their family, their lifestyle, their travel plans, and so forth". Interestingly, we found that 12.5% of the U.S. sample were "information sellers". However, our evidence is that information sellers demand a great deal more than "5 cents off." Indeed, this point distinguishes our analysis from opinion surveys: we can estimate the dollar amount that information sellers must be paid for their information.

Further, our analysis revealed a cluster that Westin (2001) did not identify. This cluster consisted of convenience seekers, people who would "sell" their personal information for convenience rather than money. Finally, among the remainder of the U.S. population, Westin (2001) differentiated between "privacy pragmatists" (63%) and "privacy fundamentalists" (25%) according to their sensitivities to privacy, while our cluster analysis did not find such a distinction. We did detect some evidence among the U.S. subjects that the privacy guardians could be further segmented, with each sub-segment placing relatively greater weight on one of the three privacy concerns.

Having identified three clusters, we investigated whether cluster membership depended systematically on particular demographic variables. We first sought systematic differences between information sellers and privacy guardians. Among the U.S. subjects, we found that information sellers had significantly more prior experience of providing personal information to websites than privacy guardians (t = 3.115, p < 0.01). The information sellers' greater prior experience was consistent with their relatively high part-worths for money. However, among the Singapore subjects, there was no significant difference between information sellers and privacy guardians in terms of prior experience of providing personal information to websites.

---

[12] Interestingly, our finding that the subjects were sensitive to convenience seems to be due solely to the convenience seekers.

We next investigated systematic differences between convenience seekers and privacy guardians. Among the U.S. subjects, convenience seekers were much more accepting of cookies than privacy guardians (t = 4.282, p < 0.001). Specifically, the convenience seekers were less concerned about cookies, and they typically accepted all cookie manipulations from websites without warning. By contrast, the majority of the privacy guardians requested to be warned about cookies. Many of them even configured their browsers to reject all cookies. The convenience seekers' greater acceptance of cookies was consistent with their relatively high part-worths for visit frequency/time savings.

Among the Singapore subjects, the convenience seekers were also less concerned about the use of cookies than the privacy guardians (t = 6.954, p < 0.001). This result was consistent with the preferences of the U.S. sample.

Overall, we found some evidence that information sellers had more prior experience of information provision than privacy guardians, and strong evidence that convenience seekers were more accepting of cookies than privacy guardians.

6. Policy and Business Implications

We now address the key public policy issue – whether the benefit of increased privacy regulation justifies the cost. In the United States, the national cost of complying with various legislative proposals to increase regulation of online privacy has been estimated to be US$9-36 billion (Hahn 2001).

Referring to Table 3, we estimate that, on average, each individual values protection against errors, improper access, and secondary use of personal information at between US$30.49 – 44.62. In March 2001, an estimated 58 million Americans made a purchase over the Internet (Horrigan and Rainie 2002). Based on the number of purchasers, we estimate the benefit of privacy protection to be US$1.77 – 2.59 billion, which falls quite far short of Hahn's (2001) cost estimates.[13] This estimate is conservative, hence understates the value of privacy protection for several reasons. Stronger privacy legislation might raise consumer participation in Internet commerce, hence generating additional benefit. Further, our calculation assumes that each

---

[13] If each person values privacy at US$30.49, then 58 million persons would value privacy at a total of 58 x 30.49 = US$1,768 million or approximately US$ 1.77 billion. Similarly, if we use the higher estimate of the value of privacy (US$44.62), the value of privacy to the entire population is US$2.59 billion.

consumer provides information to just one website. To the extent that they provide information to multiple websites, the value of privacy protection would be greater.

Our results also address another public-policy issue – the viability of proposals to regulate privacy through markets (Laudon 1996; Varian 1997). Given that individuals' concern for privacy is not absolute, but rather can be traded off against benefits such as money and convenience, we conclude that market solutions may well be viable.

As for business implications, we identified three distinct segments – privacy guardians, information sellers, and convenience seekers – in terms of individual trade-offs between the benefits of disclosing personal information and privacy concerns. The immediate implication is that e-commerce providers must differentiate their services to serve these distinct segments. Just as an auto manufacturer makes differentiated models for various segments, an e-commerce provider must differentiate its services to best meet the needs of segments with differing trade-offs among money, convenience, and privacy concerns.

Convenience seekers will be the first to register with a website if it simplifies web site navigation or enables personalized content. Businesses can exploit this by offering them the opportunity to provide personal information to customize the web site and simplify the shopping experience.

Information sellers are distinguished from privacy guardians by prior experience of information provision. This customer type cannot be lured to provide personal information by offering them convenience. To the extent that businesses cannot observe a consumer's prior experience, they must use indirect methods to induce segmentation by self-selection (Bhargava and Choudhary 2002; Moorthy 1984; Png 2002, Chapter 9). Businesses could use monetary rewards to attract information sellers to provide personal information. Preferably, businesses would seek convenience seekers first before enticing information sellers.

By elimination, the consumers who do not respond to either monetary reward or convenience would be privacy guardians. Businesses would need to use other strategies, such as privacy seals (Benassi 1999) or procedural fairness (Culnan and Armstrong 1999), to persuade these consumers to provide their personal information.

7. <u>Concluding Remarks</u>

By applying conjoint analysis, we have shown that individuals' preferences over disclosing personal information to websites do systematically vary with monetary reward and convenience. Further, we provided the first analysis of the benefit vis-à-vis cost of increased privacy regulation in the United States. In addition, we identified three distinct segments in terms of individual trade-off between the benefits of disclosing personal information and privacy concerns – privacy guardians, information sellers, and convenience seekers. Finally, we made some headway in characterizing these segments.

Our findings are subject to a number of limitations which are common to many experimental settings. All of our subjects were undergraduate students. They would be younger and probably be more familiar with the Internet and e-commerce than the general consumer population. Further, they may have had relatively little experience of medical problems, relatively little travel experience, and had too little wealth to be familiar with investment opportunities and risks. This might explain why we found no systematic industry differences in subjects' preferences.[14] For all these reasons, it would be important to verify our findings with a more representative sample of subjects.

We tested our hypotheses using experimental data collected from Singapore and U.S. subjects, which include students from diverse countries and cultures. Although our results are remarkably consistent across the two samples, future work could explore the possible influences of cultural values on individuals' preferences for privacy and positive reinforcements. Previously, using Hofstede's (1991) cross-cultural value indices, Milberg et al. (2000) find that privacy concern is positively related to power distance, individualism and masculinity, and negatively related to uncertainly avoidance. We do not have a priori information or checking on the cultural values of our subjects. Therefore, it is infeasible for us to interpret our results in light of cultural differences. It would be interesting for future research to extend our findings and introduce cultural factors when studying decisions involving privacy trade-offs.

Further, the reported part-worths are sensitive to the specified attribute levels. For example, our conjoint stimuli specified only two levels of each privacy concern – no protection and protection. In reality, however, businesses have more flexibility. For example, they may

20

state that personal information is currently not used for secondary purposes, but that such a practice cannot be ruled out in the future. Similarly, rewards may range from cash or vouchers to lottery drawings. Different reward structures may imply different estimates for the marginal utility of a one-dollar reward. Future research may attempt to measure the impact of privacy policies and reward structures more directly.[15]

---

[14] By contrast, Westin (2001) reported that Americans were particularly sensitive to privacy over financial and health information.

[15] However, this may require a willingness of the businesses to share the kind of data that they have promised not to share for secondary use.

21

References

Addelman, Sidney "Orthogonal Main-Effect Plans for Asymmetrical Factorial Experiments," *Technometrics*, vol.4, no.1, February 1962.

Alderson, Wroe and Miles W. Martin "Toward a Formal Theory of Transacations and Transvections," Journal of Marketing Research, 2 (May), 1965, pp. 117-127.

Bagozzi, Richard P. "Marketing as Exchange," Journal of Marketing, 39 (October), 1975, pp. 32-39.

Becker, Gary S. "A Theory of the Allocation of Time," *The Economic Journal*, vol. 75, no. 299, September 1965, pp. 493-517.

Benassi, Paola "Truste: An Online Privacy Seal Program," *Communications of the ACM*, vol. 42, no. 2, February 1999, pp. 56-59.

Bhargava, H.K. and V. Choudhary "One Size Fits All? Optimality Conditions for Versioning and Second-degree Price Discrimination," Pennsylvania State University, March 2002.

Blau, Peter M. *Exchange and Power in Social Life*. John Wiley & Sons, Inc. 1964.

Brinberg, David and Ronald Wood "A Resource Exchange Theory Analysis of Consumer Behavior," *Journal of Consumer Research*, vol. 10, no. 3, December 1983, pp. 330-338.

Chellappa, Ramnath and Sin, Raymond "Personalization versus Privacy: New Exchange Relationships on the Web," Working Paper, ebizlab, Marshall School of Business, USC, May 2002.

Cox, Donald F. and Stuart U. Rich "Perceived Risk and Consumer Decision-Making: the Case of Telephone Shopping," *Journal of Marketing Research*, vol. 1, November 1964, pp. 32-39.

Cranor, Lorrie Faith, Joseph Reagle and Mark S. Ackerman "Beyond Concern: Understanding Net Users' Attitudes About Online Privacy," *AT&T Labs-Research Technical Report* TR 99.4.3, 1999. http://www.research.att.com/library/trs/TRs/99/99.4/

Culnan, Mary J. "How Did They Get My Name? An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use," *MIS Quarterly*, vol. 17, no. 3, September 1993, pp. 341-363.

Culnan, Mary J. and Pamela K. Armstrong "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science*, vol. 10, no. 1, January-February 1999, pp. 104-115.

22

Donnenwerth, Gregory V. and Uriel G. Foa "Effect of Resource Class on Retaliation to Injustice in Interpersonal Exchange," *Journal of Personality and Social Psychology*, vol. 29, no. 6, 1974, pp. 785-793.

Dowling, Grahame R. and Richard Staelin "A Model of Perceived Risk and Intended Risk-handling Activity," *Journal of Consumer Research*, vol. 21, no. 1, June 1994, pp. 119-134.

Eddy, Erik R., Dianna L. Stone and Eugene F. Stone-Romero "The Effects of Information Management Policies on Reactions to Human Resource Information Systems: An Integration of Privacy and Procedural Justice Perspectives," *Personnel Psychology*, vol. 52, 1999, pp. 335-358.

Emerson, Richard M. "Exchange Theory Part I: A Psychological Basis for Social Exchange," in *Social Theories in Progress*, eds. Joseph Berger, Morris Zelditch, Jr., Bo Anderson, Houghton Mifflin Company, 1972a, pp. 38-57.

Emerson, Richard M. "Exchange Theory Part II: Exchange Relations and Network Structures," in *Social Theories in Progress*, eds. Joseph Berger, Morris Zelditch, Jr., Bo Anderson, Houghton Mifflin Company, 1972b, pp. 58-87.

Esrock, Stuart L. and John P. Ferre "A dichotomy of privacy: Personal and professional attitudes of marketers," *Business and Society Review*, vol. 104, no. 1, Spring 1999, pp. 107-120.

European Union, Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (95/46/EC), 1995.

Foa, Uriel G. "Interpersonal and Economic Resources," *Science*, vol. 171, 1971, pp. 345-351.

Friedman, M. and L.J. Savage "The utility analysis of choices involving risk," *Journal of Political Economy*, vol. 56, no. 4, August 1948, pp. 279-304.

Goodwin, Cathy "Privacy: Recognition of a Consumer Right," *Journal of Public Policy and Marketing*, vol. 10, no. 1, Spring 1991, pp. 149-166.

Goodwin, Cathy "A Conceptualization of Motives to Seek Privacy for Nondeviant Consumption," *Journal of Consumer Psychology*, vol. 1, no. 3, 1992, pp. 261-284.

Green, Paul E. and Abba M. Krieger "Segmenting Markets with Conjoint Analysis," *Journal of Marketing*, vol. 55, no. 4, October 1991, pp. 20-31.

Green, Paul E. and V. Srinivasan "Conjoint Analysis in Marketing: New Developments With Implications for Research and Practice," *Journal of Marketing*, vol. 54, no. 4, 1990, pp.3-19.

23

Gutek, Barbara "The social psychology of service interactions" *Journal of Social Issues*, vol. <u>55,</u> no. 3, 1999, pp. 603-617.

Hahn, Robert "An Assessment of the Costs of Proposed Online Privacy Legislation," *AEI-Brookings Joint Center for Regulatory Studies*, May 2001.

Hair, Joseph F., Ronald L. Tatham, Rolph E. Anderson and William C. Black. *Multivariate Data Analysis with Readings*. Prentice Hall, 1998.

Hartley, Roger, and Lisa Farrell "Can Expected Utility Theory Explain Gambling?" *American Economic Review*, vol. 92, no. 2, June 2002, pp. 613-624.

Hirschman, Elizabeth C. "People as Products: Analysis of a Complex Marketing Exchange," *Journal of Marketing*, vol. 51, no. 1, January 1987, pp. 98-108.

Hoffman, Donna L., Novak, Thomas P. and Peralta, Marcos A. "Building Consumer Trust Online," *Communications of the ACM*, vol. 42, no. 4, April 1999, pp. 80-85.

Hofstede, Geert H. *Cultures and Organizations*. McGraw-Hill, Berkshire, England, 1991.

Homans, George Caspar. *Social Behavior: Its Elementary Forms*. Harcourt Brace Jovanovich, Inc. 1974.

Horrigan, John B. and Lee Rainie "Getting Serious Online," *Pew Internet & American Life Project*, Washington, DC, March 2002. http://www.pewinternet.org/reports/pdfs/PIP_Getting_Serious_Online3ng.pdf

Jupiter Media Metrix "Seventy Percent of US Consumers Worry About Online Privacy, But Few Take Protective Action," Press Release, June 3, 2002.

Laudon, Kenneth C. "Markets and privacy," *Communications of the ACM*, vol. 39, no. 9, 1996, pp. 92-104.

Laufer, Robert S. and Maxine Wolfe "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory," *Journal of Social Issues*, vol. 33, no. 3, 1977, pp. 22-42.

Leclerc, France, Bernd H. Schmitt and Laurette Dube "Waiting Time and Decision Making: Is Time like Money," *Journal of Consumer Research*, vol. 22, no. 1, June 1995, pp. 110-119.

Milberg, Sandra J., H. Jeff Smith and Sandra J. Burke "Information Privacy: Corporate Management and National Regulation," *Organization Science*, vol. 11, no. 1, 2000, pp. 35-57.

24

Milberg, Sandra J., Sandra J. Burke and H. Jeff Smith "Values, Personal Information Privacy, and Regulatory Approaches," *Communications of the ACM*, vol. 38, no. 12, 1995, pp. 65-74.

Milne, George R. and Mary Ellen Gordon "Direct Mail Privacy-Efficiency Trade-offs within an Implied Social Contract," *Journal of Public Policy and Marketing*, vol. 12, no. 2, Fall 1993, pp. 206-215.

Moorthy, K. Sridhar "Market Segmentation, Self-Selection, and Product Line Design," *Marketing Science*, vol. 3, no. 4, Fall 1984, pp. 288–307.

New York Times "Giving the Web a Memory Cost Its Users Privacy," September 4, 2001.

Oberndorf, Shannon "Registering for Success," *Catalog Age*, vol. 16, no. 13, 1999, pp. 47-48.

OECD. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Privacy Guidelines), 23 September 1980. http://www1.oecd.org/dsti/sti/it/secur/prod/privacyguide.htm

Phelps, Joseph, Glen Nowak and Elizabeth Ferrell "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy and Marketing*, vol. 19, no. 1, Spring 2000, pp. 27-41.

Piskorski, Mikolaj. "Reciprocity in the Venture Capital Syndication Market," Working Paper, GSB Stanford 2002

Png, Ivan. *Managerial Economics*, Malden, MA: Blackwell, 2002.

Ratchford, Brian T. "The Economics of Consumer Knowledge," *Journal of Consumer Research*, vol. 27, no. 4, March 2001, pp. 397-411.

Russell, Cheryl "Kiss and Tell," *American Demographics*, vol. 11, no. 12, December 1989, pp. 2.

Smith, H. Jeff, Sandra J. Milberg and Sandra J. Burke "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," *MIS Quarterly*, vol. 20, no. 2, June 1996, pp. 167-196.

Stewart, Kathy A. and Albert H. Segars "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research*, vol. 13, no. 1, March 2002, pp. 36-49.

Stone, Eugene F. and Dianna L. Stone "Privacy in organizations: theoretical issues, research findings, and protection mechanisms," *Research in Personnel and Human Resources Management*, vol. 8, 1990, pp. 349-411.

25

Stone, Eugene F., Hal G. Gueutal, Donald G. Gardner and Stepherd McClure "A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations," *Journal of Applied Psychology*, vol. 68, no. 3, 1983, pp. 459-468.

Thibaut, John and Harold Kelly, *The social psychology of groups.* New York, New York: Wiley, 1959.

Tolchinsky, Paul D., Michael K. McCuddy, Jerome Adams, Daniel C. Ganster, Richard W. Woodman and Howard L. Fromkin "Employee Perceptions of Invasion of Privacy: A Field Simulation Experiment," *Journal of Applied Psychology*, vol. 66, no. 3, 1981, pp. 308-313.

Turner, Michael A. "The Impact of Data Restrictions On Consumer Distance Shopping," *Direct Marketing Association*, 2001. http://www.the-dma.org/isec/9.pdf

U.S. Public Interest Research Group "Public Comment on Barriers to Electronic Commerce," *Response to call by U.S. Department of Commerce* (65 Federal Register 15898), April 25, 2000.

Varian, Hal "Economic Aspects of Personal Privacy," in U.S. Department of Commerce, *Privacy and Self-Regulation in the Information Age*, June 1997.

Vriens, Marco, Michel Wedel and Tom Wilms "Metric Conjoint Segmentation Methods: A Monte Carlo Comparison," *Journal of Marketing Research*, vol. 33, no. 1, 1996, pp. 73-85.

Ward, Michael R. "The Economics of Online Retail Markets," in Gary Madden and Scott Savage, Eds., *The International Handbook on Emerging Telecommunications Networks*, Edward Elgar Publishers, 2001.

Westin, Alan. Testimony before U.S. House of Representatives, Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection, Hearing on "Opinion Surveys: What Consumers Have To Say About Information Privacy," May 8, 2001.

Westin, Alan F. *Privacy and Freedom*, New York, NY: Atheneum, 1967.

Wittink, Dick R. "Market Measurement and Analysis: The First 'Marketing Science' Conference," *Marketing Science*, vol. 20, no. 4, Fall 2001, pp. 349-356.

Wittink, Dick R. and Philippe Cattin "Commercial Use of Conjoint Analysis: An Update," *Journal of Marketing*, vol. 53, no. 3, July 1989, pp. 91-96.

Woodman, Richard W., Daniel C. Ganster, Jerome Adams, Michael K. McCuddy, Paul D.

26

Tolchinsky and Howard Fromkin "A Survey of Employee Perceptions of Information Privacy in Organizations," *Academy of Management Journal*, vol. 25, no. 3, 1982, pp. 647-663.

27

Table 1: Descriptive Statistics

	U.S.	Singapore
Number of subjects	84	184
Percentage of females	42%	44%
Average age	24	23.1
Average Internet experience (years)	6.8	5.9
Percentage of subjects having online purchase experience	95%	61%
Subjects' country of origin (number of subjects)	U.S. (48), India (13), 10 other countries (each less than 5)	Singapore (145), Malaysia (12), 9 other countries (each less than 5)

28

Table 2. Part-Worths and Relative Importance

Instruments	Level	U.S. Part-Worth[+]	U.S. Relative Importance	Singapore Part-Worth[+]	Singapore Relative Importance
Monetary Reward	$5[#]	0	26.24%	0	11.69%
	$10[#]	1.327[***] (0.341)		0.232 (0.165)	
	$20[#]	3.141[***] (0.534)		1.388[***] (0.281)	
Visit Frequency/Time Savings	Monthly	0	6.13%	0	6.02%
	Weekly	0.568[**] (0.260)		0.432[***] (0.153)	
	Daily	0.734[*] (0.411)		0.715[***] (0.254)	
Error	No Review	0	24.80%	0	15.06%
	Review	2.968[***] (0.355)		1.787[***] (0.194)	
Improper Access	No restriction	0	25.12%	0	28.43%
	Restriction	3.007[***] (0.529)		3.374[***] (0.349)	
Unauthorized Secondary Use	Allowed	0	17.70%	0	38.80%
	Not allowed	2.118[***] (0.324)		4.605[***] (0.297)	

[+] Standard errors in parentheses. The control stimulus consisted of the lowest levels of each of the included dimensions. Because the control was represented by a least squares intercept, we label all lowest level part-worths as zero. The mean intercept is not reported for brevity.
[#] US dollars for U.S. subjects and Singapore dollars for Singapore subjects.
[***] significant at 1% level;[**] significant at 5% level;[*] significant at 10% level.

Table 3: Value of Privacy (in U.S. dollars)

Website privacy policy	Value U.S.	Value Singapore
Review for error	$11.18 - 16.36	$10.45
Restriction against improper access	$11.33 - 16.58	$19.73
Secondary use not allowed	$ 7.98 - 11.68	$26.93

29

Table 4: Clusters

Segment (no. of observations)		Average part-worth				
		Monetary reward	Visit Frequency/ Time Savings	Error	Unauthorized Secondary Use	Improper Access
U.S. (78) +	Privacy guardians (56)	1.637*** (0.385)	0.027 (0.316)	4.040*** (0.434)	2.576*** (0.448)	5.116*** (0.519)
	Information sellers (16)	10.865*** (0.330)	-0.781 (0.753)	0.245 (0.458)	1.255** (0.483)	-0.099 (0.462)
	Convenience seekers (6)	1.445 (0.781)	11.028*** (0.613)	1.500** (0.348)	0.750* (0.371)	0.542 (0.945)
Number of outliers/unclassifiable observations: 6						
Singapore (165) +	Privacy guardians (138)	0.464** (0.195)	0.089 (0.166)	2.234*** (0.183)	5.734*** (0.318)	4.973*** (0.314)
	Information sellers (14)	11.286*** (0.360)	-0.714 (0.855)	0.107 (0.263)	1.768*** (0.434)	0.446 (0.470)
	Convenience seekers (13)	1.127 (0.862)	10.512*** (0.682)	0.404 (0.372)	1.077** (0.484)	0.173 (0.382)
Number of outliers/unclassifiable observations: 19						

+ Number excluding outliers.
*** significant at 1% level; ** significant at 5% level; * significant at 10% level.
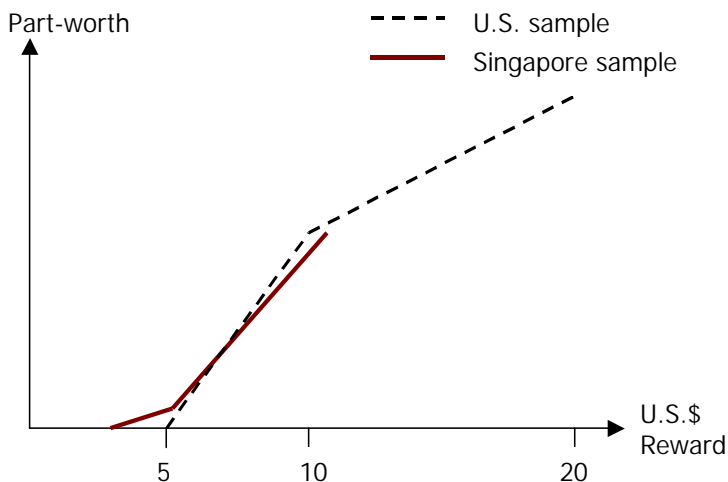Standard errors in parentheses.

Figure 1: Part-Worths for Monetary Reward

Exhibit Q

EFF TURNS 30! LEARN MORE.

California's Reader Privacy Act Signed into Law

EFF-Backed Bill Will Protect Californians' Reading Habits

PRESS RELEASES

California's Reader Privacy Act Signed into Law

Sacramento, CA – California Governor Jerry Brown has signed the Reader Privacy Act, updating reader privacy law to cover new technologies like electronic books and online book services as well as local bookstores.

The Electronic Frontier Foundation (EFF) and the American Civil Liberties Union (ACLU) were sponsors of the bill, authored by California State Senator Leland Yee. It had support from Google, TechNet and the Consumer Federation of California,

along with the Internet Archive, City Lights Bookstore, and award-winning authors Michael Chabon and Ayelet Waldman. The Reader Privacy Act will become law on January 1, and will establish privacy protections for book purchases similar to long-established privacy laws for library records.

"This is great news for Californians, updating their privacy for the 21st Century," said EFF Legal Director Cindy Cohn. "The Reader Privacy Act will help Californians protect their personal information whether they use new digital book services or their corner bookstore."

Reading choices reveal intimate facts about our lives, from our political and religious beliefs to our health concerns. Digital books and book services can paint an even more detailed picture -- including books browsed but not read, particular pages viewed, how long spent on each page, and any electronic notes made by the reader. Without strong privacy protections like the ones in the Reader Privacy Act, reading records can be too easily targeted by government scrutiny as well as exposed in legal proceedings like divorce cases and custody battles.

"California should be a leader in ensuring that upgraded technology does not mean downgraded privacy," said Valerie Small Navarro, Legislative Advocate with the ACLU's California affiliates. "We should be able to read about anything from politics, to religion, to health without worrying that the government might be looking over our shoulder."

"California law was completely inadequate when it came to protecting one's privacy for book purchases, especially for online shopping and electronic books," said Yee. "Individuals should be free to buy books without fear of government intrusion and witch hunts. If law enforcement has reason to suspect wrongdoing, they should obtain a court order for such information."

Contacts:

Cindy Cohn
Legal Director
Electronic Frontier Foundation
cindy@eff.org

Rebecca Jeschke
Media Relations Director

Electronic Frontier Foundation
press@eff.org

RELATED CASES:

READER PRIVACY ACT OF 2011

ELECTRONIC FRONTIER FOUNDATION
eff.org
Creative Commons Attribution License