S. HRG. 111–1038

CONSUMER ONLINE PRIVACY

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

JULY 27, 2010

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

67–686 PDF WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

JOHN D. ROCKEFELLER IV, West Virginia, *Chairman*

DANIEL K. INOUYE, Hawaii
JOHN F. KERRY, Massachusetts
BYRON L. DORGAN, North Dakota
BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
FRANK R. LAUTENBERG, New Jersey
MARK PRYOR, Arkansas
CLAIRE MCCASKILL, Missouri
AMY KLOBUCHAR, Minnesota
TOM UDALL, New Mexico
MARK WARNER, Virginia
MARK BEGICH, Alaska

KAY BAILEY HUTCHISON, Texas, *Ranking*
OLYMPIA J. SNOWE, Maine
JOHN ENSIGN, Nevada
JIM DEMINT, South Carolina
JOHN THUNE, South Dakota
ROGER F. WICKER, Mississippi
GEORGE S. LEMIEUX, Florida
JOHNNY ISAKSON, Georgia
DAVID VITTER, Louisiana
SAM BROWNBACK, Kansas
MIKE JOHANNS, Nebraska

ELLEN L. DONESKI, *Staff Director*
JAMES REID, *Deputy Staff Director*
BRUCE H. ANDREWS, *General Counsel*
ANN BEGEMAN, *Republican Staff Director*
BRIAN M. HENDRICKS, *Republican General Counsel*
NICK ROSSI, *Republican Chief Counsel*

CONTENTS

WITNESSES

APPENDIX

CONSUMER ONLINE PRIVACY

TUESDAY, JULY 27, 2010

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 2:36 p.m. in room SR–253, Russell Senate Office Building, Hon. John D. Rockefeller IV, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. JOHN D. ROCKEFELLER IV, U.S. SENATOR FROM WEST VIRGINIA

The CHAIRMAN. This hearing will come to order.

And I should warn our participants here that we have, I believe, a vote at 3 o'clock; originally, it was at 2:45, so we have 15 minutes of grace, some of which will be taken up by my opening statement, for which I apologize, but which I am going to enormously enjoy giving. So, thank you very much for being here. And others are trying to juggle stuff, but they will all be here.

Today, our committee is going to examine the issue of consumer privacy in an online world. Mark Pryor had a subcommittee hearing on this subject, with respect to children. But, this is actually the first time, I think, in committee's history, that we have had precisely this kind of, writ large, online privacy hearing. So, it's very important to me. It's an issue I am deeply interested in, and I know my colleagues, especially Senators Kerry and Pryor, who chair the Subcommittees on Communications Consumer Protection, are, also. I thank them for their work on this issue.

Imagine this scenario: You're in a shopping mall. And while you're there, there's a machine recording every store you enter and every product that you look at and every product that you buy. You go into a bookstore, the machine records every book you purchase and every book you peruse. Then you go to a drugstore. The machine is watching you there, meticulously recording every product you pick up, from the shampoo and the allergy medicine to your personal prescription, if you are searching for one.

The machine records your every move that day—every single move. Then, based on what you look at, where you shop, what you buy, it builds a personality profile on you. It predicts what you may want in the future and starts sending you coupons. Further, it tells businesses what a good potential client you may be and shares your personality profile with them. Do they have your permission for doing that? Of course not. Is it possible that they give you some alternatives, in fine print, which nobody has the time or the inter-

est or the eyesight to read? They might, but that doesn't count, if we're doing this straight up.

So, this sounds fantastic, something like out of a science fiction. But, this fantastic scenario is essentially what happens every second of every day to anyone who uses the Internet. Every time you go online, a computer server tracks the websites that you visit. When you send or receive an e-mail, a computer may scan the contents of that e-mail. And when you use a mobile device, a computer often tracks your location—very interesting—your location, where you are. Moreover, these computers—computer servers, these machines, as I call them, are storing all of this information about you and using it to build your personality profile, which, as it happens, they share with others. And thus, we enter the briar patch. From this profile, they determine your personal tastes and private characteristics. They inundate you with advertisements based on this information. They can spam and potentially scam you.

So, the questions we ask today are: Do consumers know what these online practices do? Are they—do they have a sense of awareness about this? Do consumers realize that computers are tracking what streets they walk on and what websites they visit? If they're not, is that important? Do they realize that the information they put on their personal websites is being shared with third parties? That wouldn't occur to a lot of teenagers. And what are consumers getting in exchange for this information-sharing, to which they have not given consent? Some can argue, "Well, the fine print is there, and it's not our fault that you didn't read it." I say that's a 19th-century argument, not one suitable for the 21st century or for honest relations with customers.

We must also ask: If consumers fully understand just what was being collected and shared about them, what could they do to stop it? Is there an opt-out? Is it in fine print? Is it visible? Do they have this choice, to stop it? Consumers demand the same degree of anonymity on the Internet that they have in a shopping mall? Fair question.

I want to close by emphasizing an important point. The consumer I'm concerned about is not a savvy computer whiz kid. I'm not talking about a lawyer who reads legalese for a living and can delve into fine print of what privacy protections he or she is getting. I am talking about ordinary Internet users. I'm talking about a 55-year-old coal miner in West Virginia who sends an e-mail to his son in college, where he is very proud that he is studying. I'm talking about a 30-year-old mother who uses her broadband connection to research the best doctor she can take her sick toddler to see. I'm talking about a 65-year-old man who has just signed up for a Facebook account so he can view photos of his grandson and reconnect with old friends.

We have a duty to ask whether these people, and the millions of Americans just like them, fully understand and associate what information is being collected about them, and whether or not they're empowered to stop certain practices from taking place.

We have two terrific panels of witnesses today. I want to thank those two chairmen before me, and the others who will follow, for spending their time with us.

Senator Hutchison is not here. This is an extraordinarily important hearing—groundbreaking, I hope; and problem solving, I hope. So, I would ask any of my colleagues—Senator Warner, do you have a statement you would like to make?

Senator WARNER. No comments at this time.

The CHAIRMAN. Absolute silence from the Committee?

STATEMENT OF HON. MIKE JOHANNS, U.S. SENATOR FROM NEBRASKA

Senator JOHANNS. Mr. Chairman, your comments were so good; I want to associate myself with them. Most importantly, I want to say thank you for conducting this hearing.

You can see, by the turnout, that obviously people are interested in this topic. I don't like the sounds of what you describe, just to be very blunt about it. And I am hoping the witnesses, as they parade before us, can soothe my fears here about how much people know about my background just because I choose to use a certain search engine.

And so, I think maybe it's time to just go to the witnesses. But, excellent opening comment.

The CHAIRMAN. I added, with amusement, a comment. My wife and I have four children. They're all between 30 and 40 years old. They're all really good on the computer. Not as good as the two witnesses at the table, but pretty close. And I told them about the hearing we were having today. They were shocked, "How can you do that? This is the future?" and, "These are great companies," et cetera, et cetera. So, I left my hearing book with them, including my statements and the explanations, questions and all that kind of thing. And they said, "Well, we're busy right now." I said, "Well, just return it to my door before dawn," which they did. So, that goes in the record.

[Laughter.]

The CHAIRMAN. Julius Genachowski, do you want to start?

STATEMENT OF HON. JULIUS GENACHOWSKI, CHAIRMAN, FEDERAL COMMUNICATIONS COMMISSION

Mr. GENACHOWSKI. I'm happy to.

Mr. Chairman, members of the Committee, thank you for this opportunity to discuss the important issue of consumer privacy.

Privacy is central to our Nation's values and way of life. And the FCC has long worked to protect the privacy of consumers who rely on our Nation's communications infrastructure. Privacy has deep intrinsic value. It is also critical for promoting investment, innovation, and adoption of cutting-edge communications technologies that bolster our economy, promote our global competitiveness, and improve our daily lives. When consumers fear that privacy is at risk, they are less likely to use new communications technologies and services.

The Commission's National Broadband Plan concluded that even as consumers learn the benefits of Internet connectivity, they are rightly concerned about privacy online. The plan also discusses how both consumers and companies can benefit from innovative personalized services based on an appropriate use of consumer information.

The plan that's recognized is that promoting both broadband and consumer privacy are key to harnessing the opportunities of the Internet. Among the Commission's key principles, when it comes to privacy, are to ensure that consumers—ordinary consumers—are empowered to control how their information is used, that providers are transparent about their practices, and that personal data is secured in a way that protects consumers, including from malicious third parties.

The Communications Act includes provisions on consumer privacy relating to telecommunications carriers, cable and satellite companies. And the Commission has extended privacy protections to consumers of interconnected voice-over-IP services.

The Commission has been active in enforcing the consumer privacy rules under our jurisdiction. In just the last year, the Commission took action against nearly 300 companies that failed to certify their compliance with our privacy rules, actions against these telecommunications carriers that ranged from issuing notices of apparent liability to imposing fines.

The Commission has also adopted rules and worked with the Federal Trade Commission to implement the Do Not Call law, to protect consumers from unsolicited calls, and has adopted rules to prohibit junk faxes. In 2009, the Commission has enforced these provisions against over 400 companies. Historically, the Commission has also worked with the FTC to prevent pre-texting.

As telephone and cable companies increasingly provide broadband services, they have growing access to significant and sensitive consumer information. In this regard, the National Broadband Plan reviewed the current regulatory landscape regarding online privacy and found that the existing framework, in some cases, is confusing and would benefit from increased clarity.

The Broadband Plan recommended that the FCC work closely on these issues with the Federal Trade Commission. I'm pleased to report that, as recommended by the Broadband Plan, our agencies have formed a joint task force to develop effective and coordinated approaches to protecting online privacy.

We're currently working together on education and transparency initiatives to help inform and empower consumers. The FCC is a leading member of OnGuard Online, a coalition of private and private—public and private organizations, spearheaded by the FTC, that provides advice to consumers on protecting their personal information. The FTC has shown consistent leadership here.

And, as part of the FCC's focus on consumers, the agency is, today, launching a new online consumer help center. This website will allow consumers to easily access the many resources that the FCC has developed to help consumers, including with respect to privacy issues, such as a consumer-friendly system for filing complaints; and news, information, and advice for consumers.

The National Broadband Plan also emphasized that our networks are vulnerable to cyber attacks that can expose personal information. In this regard, the FCC recently began an inquiry on the merits of establishing a certification program for cybersecurity standards and best practices as part of its work on privacy and security.

As we continue to move forward in online privacy, security, and other vital issues, it is important that uncertainties in the regu-

latory framework be resolved. What matters most is the consumer. I look forward to working with the Committee on these issues. And I look forward to your questions.

[The prepared statement of Mr. Genachowski follows:]

PREPARED STATEMENT OF HON. JULIUS GENACHOWSKI, CHAIRMAN, FEDERAL COMMUNICATIONS COMMISSION

Mr. Chairman, Ranking Member Hutchison, members of the Committee, thank you for this opportunity to discuss the important issue of consumer privacy.

The right to privacy is central to our Nation's values and way of life, and the Federal Communications Commission has long worked to implement Congress's directive to protect the privacy of consumers who rely on our Nation's communications infrastructure.

The Commission also recognizes that privacy has more than intrinsic value: it is critical for promoting investment, innovation, and adoption of cutting edge communications technologies and services that bolster our economy, promote our global competitiveness, and improve our daily lives. When consumers fear that their privacy is at risk, they are less likely to use new means of communication.

As the National Broadband Plan that the FCC sent to Congress in March recognizes, even as consumers learn the benefits of Internet connectivity, they are rightly concerned about their privacy online. Consumers are concerned about third parties having access to, and potentially misusing, sensitive information about their online activities, including website visits and searches, e-mail messages, geographic location, health records, energy usage, and purchasing history.

At the same time, the National Broadband Plan explains that both consumers and companies can benefit from innovative personalized services based on an appropriate use of consumer information. In the digital economy, digital identities can potentially be beneficial, if consumers are empowered and private information is safeguarded.

The Plan thus recognizes that promoting both broadband and privacy are key to harnessing the opportunities of the Internet.

The Commission's overarching goals when it comes to privacy are to ensure that consumers are empowered to control how their information is used; that providers are transparent about their practices; and that personal data is handled in a way that protects consumers, including from malicious third parties. In some respects the Internet presents unique privacy challenges, but these principles remain the starting point for protecting consumer privacy.

The Communications Act includes several key provisions on consumer privacy. Section 222, for example, requires telecommunications carriers to safeguard information about who consumers communicate with, the length of time they spend using the network, and their location when they use wired or wireless services. Sections 338 and 631 provide corresponding protections for users of services provided over cable and satellite systems. The Commission has formed an internal working group to coordinate the work of its bureaus and offices as they develop policies and take enforcement action under these provisions.

The Commission has adopted strong rules to protect consumers of traditional services, and has extended protections to consumers of interconnected Voice over IP services. In just the last year, the Commission has taken action against nearly 300 companies that failed to file timely certifications of their compliance with these rules, including issuing thirteen notices of apparent liability to repeat offenders who failed to file timely certifications for two consecutive years. The FCC also issued an Enforcement Advisory reminding companies of their obligation to file an annual certification of compliance with the CPNI rules, and settled an investigation into one carrier's privacy rule violations. The settlement includes a fine and a compliance plan designed to prevent future violations.

In addition, implementing the important "Do Not Call" provisions of the Communications Act, the Commission has worked with the FTC to protect consumers from unsolicited calls, and has adopted rules to prohibit junk faxes. Since 2009, the Commission has enforced these provisions against over 400 companies. Among other actions, the FCC has issued 14 forfeiture orders. The Commission has also collaborated with the FTC to prevent pre-texting, the practice whereby third parties attempt to gain unauthorized access to telephone subscribers' personal information.

As telephone and cable companies increasingly provide Internet access services, they continue to have access to significant and sensitive consumer information regarding customers' Internet communications. The networks operated by Internet service providers are a conduit for their customers' Internet communications, and

providers' failure to properly protect consumers' account information can result in the unintended disclosure of personal data to third parties.

The National Broadband Plan reviewed the current regulatory landscape regarding online privacy, and found that the existing framework in some cases is confusing and would benefit from increased clarity.

The Broadband Plan recommended that the FCC work closely on these issues with the Federal Trade Commission, which has strong expertise on online privacy. I am pleased to report that, as recommended by the Broadband Plan, our agencies have formed a Joint Task Force to develop innovative, effective and coordinated approaches to protecting online privacy.

We are currently working together on education and transparency initiatives to help inform and empower consumers in connection with online privacy. We are also working on strategies to help educate consumers with wireless home networks about the need to adopt encryption or other security protections to safeguard their information.

In addition, the FCC is a leading member of OnGuard Online, a coalition of public and private organizations spearheaded by the FTC that provides advice to consumers on protecting their personal information, guarding against Internet fraud, and protecting children's privacy online. Several months ago, I was pleased to join Chairman Leibowitz and Secretary of Education Arne Duncan to unveil *Net Cetera,* a guide for parents that covers a variety of issues that children face growing up in an increasingly digital world, including privacy.

And as part of its focus on consumers, the FCC is today launching a new online Consumer Help Center. This website will allow consumers to easily access the many resources that the FCC has developed to help consumers, including a consumer-friendly system for filing complaints; news about our major consumer initiatives; and tips and advisories.

The National Broadband Plan emphasized that the vulnerability of our communications networks to malicious attack—including malware and other attacks that can expose personal information—is a vital issue that is appropriately receiving broader and more focused attention. This October, the Commission will work closely with the FTC and other Federal agencies to launch a consumer education campaign for National Cybersecurity Awareness Month.

The FCC recently began an inquiry into whether we should establish a certification program under which service providers could be certified for their compliance with specific cybersecurity standards and best practices.

As we move forward on online privacy, cybersecurity, and other vital issues, it is important that uncertainties in the regulatory framework be resolved. I look forward to working with the Committee on these issues.

And I look forward to your questions.

The CHAIRMAN. Thank you very much.

Jon Leibowitz.

STATEMENT OF HON. JONATHAN D. LEIBOWITZ, CHAIRMAN, FEDERAL TRADE COMMISSION

Mr. LEIBOWITZ. Thank you. Thank you, Mr. Chairman, Senator Kerry, Senator Warner, Senator Thune, Senator LeMieux, Senator Johanns. I appreciate the opportunity to be here at this, the first full Committee privacy hearing in the Commerce Committee.

And let me begin by thanking you, Mr. Chairman and, really, this entire committee, for your support in protecting the FTC's jurisdiction to stop predatory financial practices as part of the financial reform legislation.

Let me also note how pleased I am to be here with my friend and colleague Julius Genachowski.

Consumer privacy has been a key FTC priority for the past two decades. Our privacy program operates on two main tracks: enforcement and policy development.

On the enforcement front, one of our most successful privacy initiatives has been the "Do Not Call Registry," which has given Americans some peace and quiet during their dinner hour, and

which the humorous Dave Barry called, "The most successful government program since the Elvis stamp." We vigorously enforce the requirements of the registry. We brought more than 64 actions alleging violations of the "Do Not Call" rule. And, just this month, the Do Not Call Registry surpassed 200 million telephone numbers—200 million. We think that might make us almost as popular, perhaps even more popular, than the Elvis stamp.

Another enforcement priority is data security, where we have brought dozens of cases. Just today, we announced our latest data security case, this one against Rite Aid. Our complaint alleges that Rite Aid violated FTC Act by, among other things, throwing away personal, private health information, financial information, and employment records into open dumpsters, where anyone could find them and take what they wanted. Our order requires Rite Aid to maintain reasonable data security and independent security audits every 2 years for the next 20 years. Rite Aid has also agreed to pay a million dollars to resolve HHS allegations that it violated HIPAA.

Let me now turn to policy development. Over the years, we've hosted workshops, we've issued reports, and encouraged self-regulation on privacy issues. For example, last year we released a report setting forth principles to guide self-regulatory efforts in the area of behavioral advertising. The report was a catalyst for a number of private-sector initiatives. And, while these initiatives are in their formative stages, they are encouraging.

More broadly, over the last few months we've hosted a series of roundtables examining consumer privacy in light of changing technologies and business models, including social networking, cloud computing, and mobile devices. We intend to release a public report on the roundtables, later this year, containing additional recommendations in three main areas:

First, many roundtable participants stated that companies should begin to bake in, or incorporate, privacy protections into their everyday business practices, such as reasonable security and data accuracy. This is sometimes known as "privacy by design." We'd like to further explore how to encourage companies to implement this concept.

Second, the FTC is considering how to simplify the privacy choices presented to consumers. One way would be to recognize that consent may not be needed for certain commonly accepted business practices. So, for example, it may be unnecessary, and even distracting, to ask a consumer to consent to sharing his or her address information with a shipping company for purposes of shipping a product, like a book from Amazon that he or she may have requested. By eliminating the need for choice for these practices, consumers can focus on the choices that really matter.

Another way to simplify choice is to present it at a time and place when the consumer is making a decision about his or her data, rather than a long, small-print, difficult-to-read, multiple-clicks-away privacy policy. It may also be useful to have some consistency and simplicity in the way that choices are presented so that consumers aren't constantly bombarded with having to make choices.

To this end, one idea we may explore, in the context of behavioral advertising, is a Do Not Track mechanism that's more com-

prehensive and easier to use than the procedures currently available, usually through a browser. Under such a mechanism consumers could opt-out of behavioral advertising more easily, rather than having to make choices on a web-site-by-web-site basis.

Third idea from the roundtables involves increasing transparency about privacy. For example, privacy policies could use standard formats so that consumers could compare privacy protections offered by different companies, and companies could sort of compete on their ability to protect privacy. The Commission is also considering how to best improve transparency in the data broker industry.

One final item before I conclude. We have a long history of working cooperatively with the FCC, including, most recently, on the net neutrality proceedings in National Broadband Plan. In connection with that work, we're, today, announcing a joint FCC/FTC task force to implement the privacy recommendations of the National Broadband Plan. But, to further our ability to work together, we renew our longstanding request to repeal the anachronistic common-carrier exemption in the FTC Act. Repeal of the common-carrier exemption would not affect the FCC's ability to protect consumers, but it would ensure that both agencies are able to work collaboratively to best protect consumers.

Let me thank you for the opportunity to appear here today. We look forward to working with this committee, and are happy to take questions.

[The prepared statement of Mr. Leibowitz follows:]

PREPARED STATEMENT OF HON. JONATHAN D. LEIBOWITZ, CHAIRMAN, FEDERAL TRADE COMMISSION

Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee, I am Jon Leibowitz, Chairman of the Federal Trade Commission ("FTC" or "Commission"). I appreciate the opportunity to present the Commission's testimony on privacy.[1]

Privacy has been central to the Commission's consumer protection mission for more than a decade. Over the years, the Commission has employed a variety of strategies to protect consumer privacy, including law enforcement, regulation, outreach to consumers and businesses, and policy initiatives.[2] In 2006, recognizing the increasing importance of privacy to consumers and a healthy marketplace, the FTC established the Division of Privacy and Identity Protection, which is devoted exclusively to privacy-related issues.[3]

Although the FTC's commitment to consumer privacy has remained constant, its policy approaches have evolved over time. This testimony describes the Commission's efforts to protect consumer privacy over the past two decades, including its two main policy approaches: (1) promoting the fair information practices of notice, choice, access, and security (the "FTC Fair Information Practices approach"); and (2) protecting consumers from specific and tangible privacy harms (the "harm-based approach"). It then discusses recent developments, including the FTC staff's Privacy Roundtables project—a major initiative to re-examine traditional approaches to privacy protection in light of new technologies and business models. Next, it sets forth some preliminary suggestions for moving forward on consumer privacy issues. It concludes by discussing our proposal to repeal the common carrier exemption for telecommunications providers.

---

[1] This written statement represents the views of the Federal Trade Commission. My oral presentation and responses are my own and do not necessarily reflect the views of the Commission or of any Commissioner.

[2] Information on the FTC's privacy initiatives generally may be found at *http://www.ftc.gov/privacy/index.html*.

[3] Prior to 2006, the Commission's Division of Financial Practices worked on privacy issues in addition to enforcing laws related to mortgage transactions, debt servicing, debt collection, fair lending, and payday lending. A different division was responsible for identity theft.

I. The FTC's Efforts to Protect Consumer Privacy

The FTC has a long track record of protecting consumer privacy. The Commission's early work on privacy issues dates back to its initial implementation in 1970 of the Fair Credit Reporting Act ("FCRA"),[4] which includes provisions to promote the accuracy of credit reporting information and protect the privacy of that information. With the emergence of the Internet and the growth of electronic commerce beginning in the mid-1990s, the FTC expanded its focus to include online privacy issues. Since then, both online and offline privacy issues have been at the forefront of the Commission's agenda, as discussed in greater detail below.

A. The FTC's Fair Information Practices Approach

Beginning in the mid-1990s, the FTC began addressing consumer concerns about the privacy of personal information provided in connection with online transactions. The Commission developed an approach by building on earlier initiatives outlining the "Fair Information Practice Principles," which embodied the important underlying concepts of transparency, consumer autonomy, and accountability.[5] In developing its approach, the FTC reviewed a series of reports, guidelines, and model codes regarding privacy practices issued since the mid-1970s by government agencies in the United States, Canada, and Europe. From this work, the FTC identified four widely accepted principles as the basis of its own Fair Information Practices approach: (1) businesses should provide *notice* of what information they collect from consumers and how they use it; (2) consumers should be given *choices* about how information collected from them may be used; (3) consumers should be able to *access* data collected about them; and (4) businesses should take reasonable steps to ensure the *security* of the information they collect from consumers. The Commission also identified *enforcement*—the use of a reliable mechanism to impose sanctions for noncompliance with the fair information principles—as a critical component of any self-regulatory program to ensure privacy online.[6]

To evaluate industry's compliance with these principles, the Commission examined website information practices and disclosures; conducted surveys of online privacy policies, commented on self-regulatory efforts, and issued reports to Congress. In 2000, the Commission reported to Congress that, although there had been improvement in industry self-regulatory efforts to develop and post privacy policies online, approximately one-quarter of the privacy policies surveyed addressed the four fair information practice principles of notice, choice, access, and security.[7] A majority of the Commission concluded that legislation requiring online businesses to comply with these principles, in conjunction with self-regulation, would allow the electronic marketplace to reach its full potential and give consumers the confidence they need to participate fully in that marketplace.[8]

Although Congress did not pass the legislation recommended by the Commission, the Commission's efforts during this time, particularly its surveys, reports, and workshops, were widely credited with raising public awareness about privacy and leading companies to post privacy policies for the first time.[9] The Commission also encouraged self-regulatory efforts designed to benefit consumers, such as the development of best practices, improvements in privacy-enhancing technologies, and the creation of online privacy certification programs.

The Commission also brought law enforcement actions to hold companies accountable for their privacy statements and practices. In February 1999, for example, the Commission alleged that GeoCities, one of the most visited websites at the time, had misrepresented the purposes for which it was collecting personal information from both children and adults.[10] In 2000, the Commission challenged a website's at-

---

[4] 15 U.S.C. §§ 1681e–i.

[5] This work included the Department of Health, Education, and Welfare's 1973 report, *Records, Computers, and the Rights of Citizens*, available at *http://aspe.hhs.gov/datacncl/1973privacy/c7.htm*, and the Organisation for Economic Cooperation and Development's 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available at *http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.*

[6] *See* Federal Trade Commission, Privacy Online: A Report to Congress (June 1998), available at *http://www.ftc.gov/reports/privacy3/priv-23.shtm*.

[7] *See* Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace (May 2000) at 13–14, available at *http://www.ftc.gov/reports/privacy2000/privacy2000.pdf*.

[8] *Id.* at 36–38.

[9] In 1999, Congress also passed the Gramm-Leach Bliley-Act, 15 U.S.C. §§ 6821–27, requiring all financial institutions to provide notice of their data practices and choice for sharing data with third parties.

[10] *In the Matter of GeoCities, Inc.*, FTC Docket No. C–3850 (Feb. 5 1999) (consent order).

tempts to sell personal customer information, despite the representation in its privacy policy that such information would never be disclosed to a third party.[11] These cases stressed the importance of keeping promises about the use of consumer information and demonstrated the Commission's commitment to protecting online privacy.

B. The Harm-Based Approach

In the early 2000s, the FTC de-emphasized its fair information practices approach as the primary means of addressing privacy issues, and shifted its focus to a "harm-based approach" for protecting consumer privacy. The approach was designed to target harmful uses of information—those presenting risks to physical security or economic injury, or causing unwarranted intrusions in our daily lives—rather than imposing costly notice and choice for all uses of information.[12] The Commission's privacy agenda began to focus primarily on: (1) data security enforcement; (2) identity theft; (3) children's privacy; and (4) protecting consumers from spam, spyware, and telemarketing.

1. Data Security Enforcement

Maintaining and promoting data security in the private sector has been a key component of the FTC's privacy agenda. Through its substantial record of enforcement actions, the FTC has emphasized the importance of maintaining reasonable security for consumer data, so that it does not fall into the hands of identity thieves and other wrongdoers.

The FTC enforces several laws with data security requirements. The Commission's Safeguards Rule under the Gramm-Leach-Bliley Act, for example, contains data security requirements for financial institutions.[13] The FCRA requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information,[14] and imposes safe disposal obligations on entities that maintain consumer report information.[15] In addition, the Commission enforces the FTC Act's prohibition against unfair or deceptive acts or practices in cases where a business makes false or misleading claims about its data security procedures, or where its failure to employ reasonable security measures causes or is likely to cause substantial consumer injury.[16]

Since 2001, the Commission has used its authority under these laws to bring 29 cases alleging that businesses failed to protect consumers' personal information.[17]

---

[11] *FTC* v. *Toysmart.com LLC*, 00–CV–11341–RGS (D. Mass. filed July 10, 2000). *See also In the Matter of Liberty Fin. Cos.*, FTC Docket No. C–3891 (Aug. 12, 1999) (consent order) (alleging that site falsely represented that personal information collected from children, including information about family finances, would be maintained anonymously); *FTC* v. *ReverseAuction.com, Inc.*, No. 00–0032 (D.D.C. Jan. 10, 2000) (consent order) (alleging that online auction site obtained consumer data from competitor site and then sent deceptive, unsolicited e-mail messages to those consumers seeking their business); *FTC* v. *Rennert*, No. CV–S–00–0861–JBR (D. Nev. July 24, 2000) (consent order) (alleging that defendants misrepresented their security practices and how they would use consumer information*); In the Matter of Educ. Research Ctr. of Am., Inc.*, FTC Docket No. C–4079 (May 6, 2003) (consent order) (alleging that personal data collected from students for educational purposes was sold to commercial marketers); *In the Matter of The Nat'l Research Ctr. for College & Univ. Admissions*, FTC Docket No. C–4071 (June 28, 2003) (consent order) (same)*; In the Matter of Gateway Learning Corp.*, FTC Docket No. C–4120 (Sept. 10, 2004) (consent order) (alleging that company rented customer information to list brokers in violation of its privacy policy); *In the Matter of Vision I Properties, LLC*, FTC Docket No. C–4135 (Apr. 19, 2005) (consent order) (alleging that a service provider disclosed customer information in violation of merchant privacy policies).

[12] *See, e.g.*, Speech of Timothy J. Muris, *Protecting Consumers' Privacy: 2002 and Beyond*, Cleveland, Ohio, Oct. 4, 2001, available at *http://www.ftc.gov/speeches/muris/privisp1002.shtm*.

[13] 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b). The Federal Deposit Insurance Corporation, National Credit Union Administration, Securities and Exchange Commission, Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Office of Thrift Supervision, Secretary of the Treasury, and state insurance authorities have promulgated comparable safeguards requirements for the entities they regulate.

[14] 15 U.S.C. § 1681e.

[15] *Id.,* § 1681w. The FTC's implementing rule is at 16 C.F.R. Part 682.

[16] 15 U.S.C. § 45(a). *See, e.g., In the Matter of Microsoft Corp.*, FTC Docket No. C–4069 (Dec. 20, 2002) (consent order) (alleging deception); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C–4148 (Sept. 20, 2005) (consent order) (alleging unfairness).

[17] *See In the Matter of Twitter, Inc.*, FTC File No. 092 3093 (June 24, 2010) (consent order approved for public comment); *In the Matter of Dave & Buster's, Inc.*, FTC Docket No. C–4291(Jun. 8, 2010) (consent order); *FTC* v. *LifeLock, Inc.*, No. 2:10–cv–00530–NVW (D. Ariz. final order filed Mar. 15. 2010); *United States* v. *ChoicePoint, Inc.*, No. 1:06–CV–0198–JTC (N.D. Ga. final order filed Oct. 14, 2009); *In the Matter of James B. Nutter & Co.*, FTC Docket No.

The FTC's early enforcement actions in this area addressed deceptive privacy statements—that is, the failure of companies to adhere to the promises they made to consumers regarding the security of their personal information.[18] Since 2005, the Commission has also alleged, in appropriate cases, that the failure to maintain reasonable security is an "unfair" practice that violates the FTC Act.[19]

These cases, against well-known companies such as Microsoft, ChoicePoint, CVS, LexisNexis, and more recently, Twitter, have involved such practices as the alleged failure to: (1) comply with posted privacy policies;[20] (2) take even the most basic steps to protect against common technology threats;[21] (3) dispose of data safely;[22] and (4) take reasonable steps to guard against sharing customer data with unauthorized third parties.[23] In each case, the Commission obtained significant relief, including requiring the companies to implement a comprehensive information security program and obtain regular third-party assessments of the effectiveness of that program.[24] In some cases, the Commission also obtained substantial monetary penalties or relief.[25] The Commission's robust enforcement actions have sent a strong signal to industry about the importance of data security, while providing guidance about how to accomplish this goal.[26]

C–4258 (June 12, 2009) (consent order); *United States* v. *Rental Research Servs., Inc.*, No. 0:09–CV–00524 (D. Minn. final order filed Mar. 6, 2009); *FTC* v. *Navone*, No. 2:08–CV–001842 (D. Nev. final order filed Dec. 30, 2009); *United States* v. *ValueClick, Inc.*, No. 2:08–CV–01711 (C.D. Cal. final order Mar. 17, 2008); *United States* v. *American United Mortgage*, No. 1:07–CV–07064 (N.D. Ill. final order filed Jan. 28, 2008); *In the Matter of CVS Caremark Corp.*, FTC Docket No. C–4259 (Jun. 18, 2009) (consent order); *In the Matter of Genica Corp.*, FTC Docket No. C–4252 (Mar. 16, 2009) (consent order); *In the Matter of Premier Capital Lending, Inc.*, FTC Docket No. C–4241 (Dec. 10, 2008) (consent order); *In the Matter of The TJX Cos.*, FTC Docket No. C–4227 (July 29, 2008) (consent order); *In the Matter of Reed Elsevier Inc.*, FTC Docket No. C–4226 (July 29, 2008) (consent order); *In the Matter of Life is good, Inc.*, FTC Docket No. C–4218 (Apr. 16, 2008) (consent order); *In the Matter of Goal Fin., LLC*, FTC Docket No. C–4216 (Apr. 9, 2008) (consent order); *In the Matter of Guidance Software, Inc.*, FTC Docket No. C–4187 (Mar. 30, 2007) (consent order); *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. C–4168 (Sept. 5, 2006) (consent order); *In the Matter of Nations Title Agency, Inc.*, FTC Docket No. C–4161 (June 19, 2006) (consent order); *In the Matter of DSW, Inc.*, FTC Docket No. C–4157 (Mar. 7, 2006) (consent order); *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C–4153 (Dec. 14, 2005) (consent order); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C–4148 (Sept. 20, 2005) (consent order); *In the Matter of Nationwide Mortgage Group, Inc.*, FTC Docket No. C–9319 (Apr. 12, 2005) (consent order); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C–4133 (Mar. 4, 2005) (consent order); *In the Matter of Sunbelt Lending Servs., Inc.*, FTC Docket No. C–4129 (Jan. 3, 2005) (consent order); *In the Matter of MTS Inc.*, FTC Docket No. C–4110 (May 28, 2004) (consent order); *In the Matter of Guess?, Inc.*, FTC Docket No. C–4091 (July 30, 2003) (consent order); *In the Matter of Microsoft Corp.*, FTC Docket No. C–4069 (Dec. 20, 2002) (consent order).

[18] *See In the Matter of Guidance Software, Inc.*, FTC Docket No. C–4187 (Mar. 30, 2007) (consent order); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C–4133 (Mar. 4, 2005) (consent order); *In the Matter of Guess?, Inc.*, FTC Docket No. C–4091 (July 30, 2003) (consent order); *In the Matter of Microsoft Corp.*, FTC Docket No. C–4069 (Dec. 20, 2002) (consent order).

[19] *See In the Matter of BJ's Wholesale Club, Inc.*, File No. 042 3160 (Sept. 20, 2005) (consent order).

[20] *See, e.g., In the Matter of Premier Capital Lending, Inc.*, FTC Docket No. C–4241 (Dec. 10, 2008) (consent order); *In the Matter of Life is good, Inc.*, FTC Docket No. C–4218 (Apr. 16, 2008) (consent order); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C–4133 (Mar. 4, 2005) (consent order); *In the Matter of MTS Inc.*, FTC Docket No. C–4110 (May 28, 2004) (consent order); *In the Matter of Microsoft Corp.*, FTC Docket No. C–4069 (Dec. 20, 2002) (consent order).

[21] *See, e.g., In the Matter of Twitter, Inc.*, FTC File No. 092 3093 (June 24, 2010) (consent order approved for public comment); *In the Matter of The TJX Cos.*, FTC Docket No. C–4227 (July 29, 2008) (consent order); *In the Matter of Reed Elsevier, Inc.*, FTC Docket No. C4226 (July 29, 2008) (consent order).

[22] *See, e.g., FTC* v. *Navone*, No. 2:08–CV–001842 (final order filed D. Nev. Dec. 30, 2009); *United States* v. *American United Mortgage*, No. 1:07–CV–07064 (N.D. Ill. final order filed Jan. 28, 2008); *In the Matter of CVS Caremark Corp.*, FTC Docket No. C–4259 (June 18, 2009).

[23] *See, e.g., United States* v. *Rental Research Servs.*, No. 09 CV 524 (D. Minn. final order filed Mar. 6, 2009); *United States* v. *ChoicePoint, Inc.,* No. 1:06–CV–0198 (final order filed N.D. Ga. Oct. 14, 2009).

[24] In addition, beginning with the CVS case announced last year, the Commission has begun to challenge the reasonableness of security measures to protect employee data, in addition to customer data. *See, e.g., In the Matter of CVS Caremark Corp.*, FTC Docket No. C–4259 (Jun. 18, 2009) (consent order).

[25] *See, e.g., FTC* v. *Navone*, No. 2:08–CV–001842 (D. Nev. final order Dec. 29, 2009); *United States* v. *ChoicePoint, Inc.*, No. 1:06–CV–0198 (final order filed N.D. Ga. Oct. 14, 2009).

[26] Developments in state law have also played a major role in data security. The passage of state data breach notification laws beginning in 2003 required increased transparency for com-

Continued

2. Identity Theft

Another important part of the Commission's privacy agenda has been protecting consumers from identity theft, which victimizes millions of consumers every year. In 1998, Congress enacted the Identity Theft Assumption and Deterrence Act ("the Act"), which provided the FTC with a specific role in combating identity theft.[27] To fulfill the Act's mandate, the Commission created a telephone hotline and dedicated website to collect complaints and assist victims, through which approximately 20,000 consumers contact the FTC every week. The FTC also maintains and promotes a centralized database of victim complaints that serves as an investigative tool for over 1,700 law enforcement agencies.

The Commission also played a lead role in the President's Identity Theft Task Force ("Task Force"). The Task Force, comprised of 17 Federal agencies and co-chaired by the FTC's Chairman, was established by President Bush in May 2006 to develop a comprehensive national strategy to combat identity theft.[28] In April 2007, the Task Force published its national strategy, recommending 31 initiatives to reduce the incidence and impact of identity theft.[29] The FTC, along with the other Task Force agencies, has been actively implementing these initiatives and submitted a final report in September 2008.[30] Among other things, the Commission has trained victim assistance counselors, Federal and state prosecutors, and law enforcement officials; developed and published an Identity Theft Victim Statement of Rights; and worked closely with the American Bar Association on a pro bono legal assistance program for identity theft victims.

Finally, the Commission has worked to implement the identity theft protections of the Fair and Accurate Credit Transactions Act of 2003 (the "FACT Act").[31] Among other things, the FTC has acted aggressively to enforce consumers' right under the FACT Act to receive a free credit report every twelve months from each of the nationwide consumer reporting agencies, so they can spot incipient signs of identity theft. For example, the Commission has brought action against a company offering a so-called "free" credit report that was actually tied to the purchase of a credit monitoring service.[32]

3. Children's Privacy

The Commission has also undertaken an aggressive agenda to protect children's privacy. Since the enactment of the Children's Online Privacy Protection Act in 1998 ("COPPA") and its implementing rule,[33] the FTC has brought 15 actions against website operators that collect information from children without first obtaining their parents' consent. Through these actions, the FTC has obtained more than $3.2 million in civil penalties.[34] The Commission is currently conducting a comprehensive review of its COPPA Rule in light of changing technology, such as the increased use of mobile devices to access the Internet.[35]

4. Unwarranted Intrusions

The Commission has also acted to protect consumers from unwarranted intrusions into their daily lives, particularly in the areas of unwanted telemarketing calls,

---

panies that had suffered data breaches and thus further enhanced the Commission's data security enforcement efforts. *See, e.g.*, Cal. Civ. Code §§ 1798.29, 1798.82–1789.84 (West 2003).

[27] 18 U.S.C. § 1028 note.

[28] Exec. Order No. 13,402, 71 Fed. Reg. 27,945 (May 15, 2006).

[29] *See* The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan (2007), available at *http://www.idtheft.gov/reports/StrategicPlan.pdf* (recommending that key agencies work together to combat identity theft by strengthening law enforcement, educating consumers and businesses, and increasing the safeguards employed by Federal agencies and the private sector to protect personal data).

[30] *See* The President's Identity Theft Task Force Report (2008), available at *http://www.idtheft.gov/reports/IDTReport2008.pdf*.

[31] Pub. L. 108–159 (2003).

[32] *FTC* v. *Consumerinfo.com, Inc.*, SACV05–801AHS(MLGx) (C.D. Cal. final order filed Jan. 8, 2007).

To provide further clarity to consumers, Congress recently enacted legislation requiring entities that advertise "free" credit reports to disclose that such reports are available pursuant to Federal law at *www.annualcreditreport.com*. See Pub. L. 111–24, *codified at* 15 U.S.C.§ 1681j(g). The FTC has promulgated a rule to implement this requirement, 16 C.F.R. § 610, and announced last week that it issued eighteen warning letters to companies alleging failures to comply with the rule.

[33] 15 U.S.C. §§ 6501–6508; 16 C.F.R. Part 312.

[34] For a list of the FTC's COPPA cases, see *http://www.ftc.gov/privacy/privacyinitiatives/childrens_enf.html*.

[35] In spring 2010, the FTC announced it was seeking comment on a broad array of issues as part of its review of the COPPA Rule. *See http://www.ftc.gov/privacy/privacyinitiatives/childrens_2010rulereview.html*.

spam, and spyware. Perhaps the Commission's most well-known privacy initiative is the Do Not Call Registry, which has been an unqualified success. The Commission vigorously enforces the requirements of the Registry to ensure its ongoing effectiveness. The FTC has brought 64 actions alleging violations of the Do Not Call Rule. These actions have resulted in $39.9 million in civil penalties and $17.7 million in consumer redress or disgorgement. During the past year, the Commission has filed several new actions that attack the use of harassing "robocalls"—the automated delivery of prerecorded messages—to deliver deceptive telemarketing pitches that promise consumers extended auto warranties and credit card interest rate reduction services.[36]

In addition, since the enactment of the CAN-SPAM Act in 2003,[37] the Commission has brought dozens of law enforcement actions challenging spam, including cases involving deceptive spam, failure to honor opt-out requests, and failure to comply with requirements for adult labeling of spam messages.[38] For example, in June 2009, the FTC moved quickly to shut down a rogue Internet Service Provider ("ISP") that knowingly hosted and actively participated in the distribution of illegal spam, child pornography, and other harmful electronic content. The FTC complaint alleged that the defendant actively recruited and colluded with criminals seeking to distribute illegal, malicious, and harmful electronic content.[39] After the Commission shut down this ISP, there was a temporary 30 percent drop in spam worldwide.[40] Finally, since 2004, the Commission has brought 15 spyware cases, targeting programs foisting voluminous pop-up ads on consumers and subjecting them to nefarious programs that track their keystrokes and online activities.[41]

C. Ongoing Outreach and Policy Initiatives

While the Commission's consumer privacy models have evolved throughout the years, its activities in a number of areas have remained constant. In addition to enforcement, these include consumer and business education, research and policymaking on emerging technology issues, and international outreach.

1. Consumer and Business Education

The FTC has done pioneering outreach to business and consumers, particularly in the area of consumer privacy and data security. The Commission's well-known OnGuard Online website educates consumers about threats such as spyware, phishing, laptop security, and identity theft.[42] The FTC also developed a guide to help small and medium-sized businesses implement appropriate data security for the personal information they collect and maintain.[43]

The FTC has also developed resources specifically for children, parents, and teachers to help kids stay safe online. In response to the Broadband Data Improvement Act of 2008, the FTC produced the brochure *Net Cetera: Chatting with Kids About Being Online* to give adults practical tips to help children navigate the online world.[44] In less than 10 months, the Commission already has distributed more than 3.8 million copies of its *Net Cetera* brochure to schools and communities nationwide. The Commission also offers specific guidance for certain types of Internet services, including, for example, social networking and peer-to-peer file sharing.[45] In addition, the Commission recently launched *Admongo.gov,* a campaign to help kids better understand the ads they see online and offline.[46]

2. Research and Policymaking on Emerging Technology Issues

Over the past two decades, the Commission has hosted numerous workshops to examine the implications of new technologies on privacy, including forums on spam,

---

[36] *See, e.g., FTC* v. *Asia-Pacific Telecom, Inc.*, No. 10 CV 3168 (N.D. Ill., filed May 24, 2010).

[37] 15 U.S.C. §§ 7701–7713.

[38] Detailed information regarding these actions is available at *http://www.ftc.gov/bcp/conline/edcams/spam/press.htm*.

[39] *FTC* v. *Pricewert, LLC*, No. 09–CV–2407 (N.D. Cal. final order issued Apr. 4, 2010).

[40] *See* Official Google Enterprise Blog, Q2 2009 Spam Trends, available at *http://googleenterprise.blogspot.com/2009/07/q2-2009-spam-trends.html*.

[41] Detailed information regarding each of these law enforcement actions is available at *http://www.ftc.gov/bcp/edu/microsites/spyware/law_enfor.htm*.

[42] *See http://www.onguardonline.gov*. Since its launch in 2005, OnGuard Online and its Spanish-language counterpart Alertaena Línea have attracted nearly 12 million unique visits.

[43] *See Protecting Personal Information: A Guide For Business*, available at *http://www.ftc.gov/infosecurity*.

[44] *See* FTC Press Release, *OnGuardOnline.gov* Off to a Fast Start with Online Child Safety Campaign (Mar. 31, 2010), available at *http://www.ftc.gov/opa/2010/03/netcetera.shtm*.

[45] *See http://www.onguardonline.gov/topics/social-networking-sites.aspx*.

[46] *See* FTC Press Release, FTC Helps Prepare Kids for a World Where Advertising is Everywhere (Apr. 28, 2010), available at *http://www.ftc.gov/opa/2010/04/admongo1.shtm*.

spyware, radio-frequency identification (RFID), mobile marketing, contactless payment, peer-to-peer file sharing, and online behavioral advertising. These workshops often spur innovation and self-regulatory efforts. For example, the FTC has been assessing the privacy implications of online behavioral advertising for several years. In February 2009, the Commission staff released a report that set forth several principles to guide self-regulatory efforts in this area: (1) transparency and consumer control; (2) reasonable security and limited retention for consumer data; (3) affirmative express consent for material retroactive changes to privacy policies; and (4) affirmative express consent for (or prohibition against) the use of sensitive data.[47] This report was the catalyst for industry to institute a number of self-regulatory advances. While these efforts are still in their developmental stages, they are encouraging. We will continue to work with industry to improve consumer control and understanding of the evolving use of online behavioral advertising.

3. International Outreach

Another major privacy priority for the FTC has been cross-border privacy and international enforcement cooperation. The Commission's efforts in this area are gaining greater importance with the proliferation of cross-border data flows, cloud computing, and on-demand data processing that takes place across national borders. To protect consumers in this rapidly changing environment, the FTC participates in various international policy initiatives, including those in multilateral organizations such as the Organization for Economic Cooperation and Development (OECD) and the Asia-Pacific Economic Cooperation forum (APEC).

In APEC, the FTC actively promotes an initiative to establish a self-regulatory framework governing the privacy of data transfers throughout the APEC region. The FTC just announced that it was one of the first participants in the APEC cross-border Privacy Enforcement Arrangement, a multilateral cooperation network for APEC privacy enforcement authorities.

In a similar vein, earlier this year, the FTC, joined by a number of its international counterparts, launched the Global Privacy Enforcement Network, an informal initiative organized in cooperation with OECD, to strengthen cooperation in the enforcement of privacy laws.

Finally, the Commission is using its expanded powers under the U.S. SAFE WEB Act of 2006[48] to promote cooperation in cross-border law enforcement, including in the privacy area. The FTC has also brought a number of cases relating to the U.S.-EU Safe Harbor Framework, which enables U.S. companies to transfer personal data from Europe to the U.S. consistent with European privacy law.[49] For example, last fall, the Commission announced enforcement actions alleging that seven companies falsely claimed to be part of the Framework. The orders against six of these companies prohibit them from misrepresenting their participation in any privacy, security, or other compliance program.[50] The seventh case is still in litigation.[51]

II. Lessons Learned

Although the Commission plans to continue its ongoing enforcement, policy, and education initiatives, it recognizes that the traditional models governing consumer privacy have their limitations.

The Fair Information Practices model, as implemented, has put too much burden on consumers to read and understand lengthy and complicated privacy policies and then make numerous choices about the collection and use of their data. Indeed, privacy policies have become complicated legal documents that often seem designed to limit companies' liability, rather than to inform consumers about their information practices.

The harm-based model has principally focused on financial or other tangible harm rather than the exposure of personal information where there is no financial or

---

[47] FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising (Feb. 2009), available at *http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf*.

[48] Pub. L. No. 109–455 (2006) (codified in scattered sections of 15 U.S.C. and 12 U.S.C. § 3412(e)).

[49] Companies self-certify to the U.S. Department of Commerce their compliance with a set of Safe Harbor privacy principles. If a company falsely claims to be part of this program, or fails to abide by its requirements, the FTC can challenge such actions under its deception authority.

[50] *See In the Matter of Directors Desk LLC*, FTC Docket No. C–4281 (Jan. 12, 2010); *In the Matter of World Innovators, Inc.*, FTC Docket No. C–4282 (Jan. 12, 2010); *In the Matter of Collectify LLC*, FTC Docket No. C–4272 (Nov. 9, 2009); *In the Matter of ExpatEdge Partners, LLC*, FTC Docket No. C–4269 (Nov. 9, 2009); *In the Matter of Onyx Graphics, Inc.*, FTC Docket No. C–4270 (Nov. 9, 2009); *In the Matter of Progressive Gaitways LLC*, FTC Docket No. C–4271 (Nov. 9, 2009).

[51] *See FTC* v. *Kavarni*, Civil Action No. 09–CV–5276 (C.D. Cal. filed July 31, 2009).

measurable consequence from that exposure.[52] Yet there are situations in which consumers do not want personal information to be shared even where there may be no risk of financial harm. For example, a consumer may not want information about his or her medical condition to be available to third-party marketers, even if receiving advertising based on that condition might not cause a financial harm. In addition, some have criticized the harm-based model as being inherently reactive—addressing harms to consumers after they occur, rather than taking preventative measures before the information is collected, used, or shared in ways that are contrary to consumer expectations.[53]

In addition, there are questions about whether these models can keep pace with the rapid developments in such areas as online behavioral advertising, cloud computing, mobile services, and social networking. For example, is it realistic to expect consumers to read privacy notices on their mobile devices? How can consumer harm be clearly defined in an environment where data may be used for multiple, unanticipated purposes now or in the future?

III. The FTC Privacy Roundtables

To explore the privacy challenges posed by emerging technology and business practices, the Commission announced late last year that it would examine consumer privacy in a series of public roundtables.[54] Through these roundtables, held in December 2009, and January and March 2010, the Commission obtained input from a broad array of stakeholders on existing approaches, developments in the marketplace, and potential new ideas.[55]

The roundtables generated significant public interest. Over 200 representatives of industry, consumer groups, academia, and government agencies participated in the roundtables, and the Commission received over 100 written comments.

Several common themes emerged from these comments and the roundtable discussions. First, consumers do not understand the extent to which companies are collecting, using, aggregating, storing, and sharing their personal information. For example, as evidence of this invisible data collection and use, commenters and panelists pointed to enormous increases in data processing and storage capabilities; advances in online profiling and targeting; and the opaque business practices of data brokers,[56] which are not understood by consumers. In addition, as commenters noted, consumers rarely realize that, when a company discloses that it shares information with affiliates, the company could have hundreds of affiliates.

Second, commenters and panelists raised concerns about the tendency for companies storing data to find new uses for that data. As a result, consumers' data may be used in ways that they never contemplated.

Third, commenters and roundtable participants pointed out that, as tools to reidentify supposedly anonymous information continue to evolve, the distinction between personally identifiable information ("PII") and non-PII is losing its significance. Thus, information practices and restrictions that rely on this distinction may be losing their relevance.

Fourth, commenters and roundtable participants noted the tremendous benefits from the free flow of information. Consumers receive free content and services and businesses are able to innovate and develop new services through the acquisition, exchange and use of consumer information. Commenters and participants noted that

---

[52] *See* Speech of Timothy J. Muris, *Protecting Consumers' Privacy: 2002 and Beyond*, Cleveland, Ohio, October 4, 2001, available at *http://www.ftc.gov/speeches/muris/privisp1002.shtm*.

[53] *See* Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 Hastings L.J. 1, 5 (2003).

[54] *See* FTC Press Release, FTC to Host Public Roundtables to Address Evolving Privacy Issues (Sept. 15, 2009), available at *http://www.ftc.gov/opa/2009/09/privacyrt.shtm*.

[55] Similar efforts are underway around the world. For example, the OECD is preparing to review its 1980 Privacy Guidelines (see *http://www.oecd.org/document/39/0,3343,en_2649_34255_44946983_1_1_1_1,00.html*); the European Commission is undertaking a review of the 1995 Data Protection Directive (see *http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm*); and the International Data Protection Commissioners' Conference released a set of draft privacy guidelines (*see http://www.privacyconference2009.org/dpas_space/Resolucion/index-iden-idphp.php*). The FTC is closely following these international developments, recognizing that the market for consumer data is becoming increasingly globalized and consumer data is more easily accessed, processed, and transferred across national borders.

In addition, following the FTC roundtables, the Department of Commerce also held a workshop and issued a Notice of Inquiry on the related subject of privacy and innovation, in which the FTC has submitted a comment. *See In the Matter of Privacy and Innovation in the Information Economy*, Docket No. 100402174–0175–01, Comments of the Federal Trade Commission (June 2008), available at *http://www.ftc.gov/os/2010/06/100623ntiacomments.pdf*.

[56] Data brokers compile information about individuals and sell it to others.

regulators should be cautious about restricting such information exchange and use, as doing so risks depriving consumers of benefits of free content and services.

Fifth, commenters and roundtable participants voiced concerns about the limitations of the FTC Fair Information Practices model. Many argued that the model places too high a burden on consumers to read and understand lengthy privacy policies and then ostensibly to exercise meaningful choices based on them. Some participants also called for the adoption of other substantive data protections—including those in earlier iterations of the Fair Information Practice Principles—that impose obligations on companies, not consumers, to protect privacy. Such participants argued that consumers should not have to choose basic privacy protections, such as not retaining data for longer than it is needed, that should be built into everyday business practices.

Sixth, many commenters called upon the Commission to support a more expansive view of privacy harms that goes beyond economic or tangible harms. There are some privacy harms, these participants argued, that pose real threats to consumers—such as exposure of information about health conditions or sexual orientation—but cannot be assigned a dollar value.

Finally, many participants highlighted industry efforts to improve transparency for consumers about the collection and use of their information. At the same time, commenters questioned whether the tools are consistent and simple enough for consumers to embrace and use effectively.

IV. Next Steps

The themes that emerged through the roundtable project have led the Commission to consider several ways to improve consumer privacy. Commission staff intends to release a report later this year in which it expects to discuss several issues, as described preliminarily below.

A. Integrating Privacy Into Business Practices

Many roundtable panelists and commenters raised the importance of companies' incorporating privacy and security protections into their everyday business practices.[57] A number of roundtable participants and commenters emphasized the value of building privacy and security protections into company procedures, systems, and technologies at the outset, so that they are an integral part of a company's business model. Such protections include providing reasonable security for consumer data, collecting only the data needed for a specific business purpose, retaining data only as long as necessary to fulfill that purpose, and implementing reasonable procedures to promote data accuracy.

Panelists and commenters stated that these measures would provide consumers with substantive protections without placing the burden on them to read long notices and make cumbersome choices. The Commission also notes that many businesses already are providing these types of protections as a matter of good business practice or due to existing sectoral laws.[58] Accordingly, the Commission is exploring whether and how to encourage companies to incorporate these protections into their practices, whether there are other protections that companies should incorporate, and how to balance the costs and benefits of such protections.

B. Simplifying Choice

The Commission is also considering whether and how to simplify the privacy choices presented to consumers. One way would be to recognize that consumers do not need to exercise choice for certain commonly accepted business practices—those that fall within reasonable consumer expectations. By eliminating the need to exercise choice for these practices, consumers can focus on the choices that really matter to them, and on uses of data that they would not expect when they engage in a transaction. Simplifying choice should also reduce the burdens on businesses.

Such commonly accepted business practices may include fulfillment, fraud prevention and responding to legal process, internal analytics, and sharing data with service providers that are acting at the company's direction. For example, it may be unnecessary, and even distracting, to ask a consumer to consent to sharing his or her address information with a shipping company for purposes of shipping a product that the consumer has requested. The Commission is considering how to define these commonly accepted business practices.

---

[57] *See generally*, Privacy Roundtable Transcripts of December 7, 2009, January 28, 2010, and March 17, 2010, available at *http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/FTCindex.html* and the Privacy Roundtable public comments, available at *http://www.ftc.gov/os/comments/privacyroundtable/index.shtm*.

[58] *See* Fair Credit Reporting Act, 15 U.S.C. §§ 1681e–i; Gramm-Leach-Bliley Act, 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b); cases cited *supra* n. 17.

The Commission is also exploring—in cases where choice would be needed—how to ensure that such choice is more meaningful. For example, rather than discussing choices in a long privacy policy, it may be most effective to present choices "just-in-time," at the point when the consumer is providing the data or otherwise engaging with a company. It also may be beneficial to have greater consistency in the way that choices are presented and expressed, so that consumers can better understand and compare companies' privacy practices. In addition, the Commission is examining how best to protect and provide effective choice for the use of sensitive information, such as health, financial, children's, and location data.

C. Improving Transparency

The Commission also is considering a number of other ways to increase transparency about commercial data practices. First, the Commission believes that privacy policies should be improved. Indeed, although excessive reliance on privacy policies has been widely criticized, roundtable participants and commenters recognized the continuing value of privacy notices to promote accountability for companies. Accordingly, in its upcoming report, the Commission will discuss ways to improve the disclosures in privacy policies. One possible approach is the use of standardized terms or formats. Clearer, more standardized privacy disclosures could allow consumers to compare the privacy protections offered by different companies and potentially increase competition on privacy practices.

Second, the Commission also is considering issues related to the practice of data aggregation. Roundtable participants and commenters expressed concern that data collected for one purpose can be combined with other data and then used for purposes not anticipated by the consumer. Further, unbeknownst to many consumers, companies such as data brokers collect and sell such aggregated data on a routine basis. At the roundtables, some panelists suggested that one solution would be to give consumers access to their data as a means of improving transparency. Others discussed the costs of providing access, and suggested that, if access is provided, it should vary with the sensitivity of the data and its intended use. The Commission recognizes the significant policy issues raised by access, and is examining whether the benefits of access are commensurate with the costs of implementation. The Commission is also considering whether there are other ways to promote greater transparency about the data aggregation practices of data brokers and others.

Third, the Commission continues to believe that requiring affirmative express consent for material retroactive changes to how data will be used is an essential means of maintaining transparency.[59]

Finally, the Commission is examining the role of education in promoting greater awareness about privacy among both businesses and consumers. For example, the Commission is interested in exploring whether businesses, industry associations, consumer groups, and the government can do a better job of informing consumers about privacy. The Commission is also evaluating the roles that government agencies and trade and industry associations can play in educating the business sector.

The FTC looks forward to developing these concepts further and to working with Congress and this Committee as the agency moves forward.

V. FCC/Common Carrier Exemption Issues

In recognition of the Federal Communication Commission's ("FCC") participation in this hearing, the Commission notes that it has a long history of cooperation and coordination with the FCC in policy matters and law enforcement, including those related to privacy. For example, the FCC and FTC cooperated extensively in implementation of the National Do Not Call Registry and continue to cooperate on enforcement of the Do Not Call rules, pursuant to a Memorandum of Understanding signed by staff of the two agencies.[60] Similarly, the FCC and FTC collaborated in efforts to address concerns raised by phone pretexters obtaining consumers' calling records without authorization.[61] That tradition continues as the FCC works on implementing its National Broadband Plan.

---

[59] *See In the Matter of Gateway Learning Corp.*, FTC Docket No. C–4120 (Sept. 10, 2004) (consent order); FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising (Feb. 2009), available at *http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf*.

[60] *See* Annual Report to Congress for FY 2003 and 2004 Pursuant to the Do Not Call Implementation Act on Implementation of the National Do Not Call Registry, available at *http://www.ftc.gov/reports/donotcall/051004dncfy0304.pdf*.

[61] *See* Prepared Statement of the Federal Trade Commission Before the Committee on Energy and Commerce, U.S. House of Representatives, "Combating Pretexting: H.R. 936, Prevention of Fraudulent Access to Phone Records Act (Mar. 9, 2007), at 4, available at *http://www.ftc.gov/os/testimony/P065409CommissionTestimonReCombatingPretextingandHR936House.pdf*.

With this history of productive cooperation in mind, the FTC renews its request for repeal of the telecommunications common carrier exemption from the FTC Act. The Commission believes that repealing the exemption would better enable the FTC and FCC to work together on privacy and other issues, and to leverage their relative expertise and resources, to achieve their common goal of protecting consumers of telecommunication services.

The FTC Act exempts common carrier activities subject to the Communications Act from its prohibitions on unfair and deceptive acts or practices and unfair methods of competition.[62] This exemption dates from a period when telecommunications were provided by highly-regulated monopolies. The exemption is now outdated. Congress and the FCC have dismantled much of the economic regulatory apparatus formerly applicable to this industry. The current environment requires telecommunications firms to compete in providing telecommunications services. Removing the exemption from the FTC Act would not alter the jurisdiction of the FCC, but would give the FTC the authority to protect consumers from unfair and deceptive practices by common carriers in the same way that it protects them against other unfair and deceptive practices.

Repeal of the common carrier exemption is particularly timely as the array of communications-related services continues to expand. The FTC has a long track record of addressing competition, consumer protection, and privacy issues with respect to information, entertainment, and payment services. In addition, the FTC has procedural and remedial tools that could be used effectively to address developing problems in the telecommunications industry.[63]

FTC staff continues to work with the FCC on a number of initiatives. Repeal of the common carrier exemption will lead to further and even more productive collaboration and ensure that consumer protection interests are well protected.

VI. Conclusion

Thank you for the opportunity to provide the Commission's views on the topic of consumer privacy. We look forward to continuing to work with Congress and this committee on this important issue.

The CHAIRMAN. Thank you very much.

The vote is in 5 minutes, so I'm going to ask a question. By that time, John Kerry will have voted and come back, and he'll chair until I get back.

This is for Chairman Leibowitz. Millions of consumers go online everyday to buy books, to watch videos, and communicate with friends and family. Because they are sitting in the privacy of their homes, people think that they are not being watched, but they are. When a woman researches breast cancer online, she is not thinking that the Website she visits may be collecting data on her and shared—sharing that data with others. It would never occur to her, never occur to me, but it happens. And she should not have to worry about her online activity being shared with a prospective employer. This is not just games, here, this is—gets to be very serious stuff. People get hired or don't get hired.

I know the Federal Trade Commission plans to release a privacy report in the fall, so my questions are the following: What is the FTC—what will you present in the way of establishing base-level privacy protections for consumers that are enforceable and which you have the authority to enforce? Which leads to the second question: Are there limitations on FTC's authority that prevent you from protecting consumers' privacy?

Mr. LEIBOWITZ. Well, let me take the second question first. You know, one of the things that we pushed very hard for—and you pushed very hard for with us, in the context of financial reform—

[62] 15 U.S.C. § 44, 45(a).

[63] These tools for injured consumers include the FTC's ability to obtain, in appropriate cases, preliminary and permanent injunctions, asset freezes, restitution, and disgorgement under the FTC Act, 15 U.S.C. § 44 *et seq.*

was the ability to sanction malefactors—to fine malefactors. And we weren't able to get it this time. But, that seems to me to be a limitation. When you have a company that engages in truly inadequate data security, or a company engaged in fraud—and we go after a lot of people who are engaged in fraud—it would help to have the stronger deterrent of a civil fine. So, that would be one area where we have limitations.

On the other hand, our statute that prohibits unfair and deceptive acts or practices is pretty broad, and it is very, very useful. And we have brought more than 100 spam and spyware cases, we've brought about 30 data-security cases, and we are going to continue to do more. Protecting American consumers' privacy is one of our highest priorities.

I would say this: Going back to your opening statement, where you made an analogy to someone walking through a mall, and they're being followed by someone who's sending out information to the stores ahead, further down along the way the consumer is walking. That's a really good analogy, I think, to what is going on, on the Internet today. Because people don't really understand privacy policies and people don't understand third-party cookies, and sometimes they'll sign up for something and their Web browsing will be followed.

I will say this: For vulnerable populations and for sensitive information, we have said—and we issued a report last year—that those should be "opt-in," rather than "opt-out." And we believe very strongly in that.

Now, occasionally you can have a better opt-out policy than an opt-in policy; but, in general, in terms of informing consumers and protecting their privacy, opt-in, particularly with vulnerable populations, like teens; or sensitive information, like medical records—that's a better approach.

The CHAIRMAN. Let me ask a second question, and then I have to go.

When I do, Byron Dorgan, if you would mind—not mind taking over? Senator Kerry, who just went to vote, when he comes back, then he will chair. When I come back from voting, I will chair.

The second is, your example, that you use in your testimony, the company Game Station, quote, "bought the souls of its customers by adding a line to its terms and conditions," demonstrates how few people actually read the—licensing agreements, and privacy practices."

One, please elaborate on that.

Mr. LEIBOWITZ. Sure. I mean, one of the things that became absolutely clear to us during our roundtables this year is that there's a huge disconnect between what consumers think happens to their data and what really happens to their data; and also consumers' understanding of privacy policies. Most consumers believe that a privacy policy protects their privacy. Instead, a privacy policy delineates their rights, and their lack thereof.

There is a story about this company—I think it was called Game Station; it's a British gaming company—on April 1 of this year, they decided to put a clause in that said, "Unless you opt-out, we take possession of your immortal soul." And if you do opt-out, they game you 5 pounds sterling—about $8—as a rebate. And only 12

percent of the people opted out, because nobody else read privacy policies. And I think it was kind of a clever way to make a very disturbing point, which is that privacy policies don't generally protect consumers, and consumers don't generally read them. And that's part of the reason why we're doing this rethink of privacy.

The CHAIRMAN. Are the licensing agreements and privacy policies effective disclosures? Do they have weight?

Mr. LEIBOWITZ. Well, I would say that some do and some don't. You know, in our spyware cases—and we've brought more than a dozen spyware cases—very often they were designed to obfuscate the fact that, if you clicked on a policy, companies would do all sorts of things with your data. I think some privacy policies are actually pretty good, but the question is: What should be the rules of the road, going forward? How do we move everyone up to the right standard? That's part of the reason we're going through this process, this initiative, and writing a report. And that——

The CHAIRMAN. As well as the size of the print.

Mr. LEIBOWITZ. Yes. And one thing that we've talked about is the notion of having a box with the most important privacy principles in them, and the most important terms and conditions, so consumers will understand it. And it'll be on the first click, not the third or the fourth. And that's a good way to bake in privacy principles. And we'd like to see more of that.

The CHAIRMAN. Can you create that?

Mr. LEIBOWITZ. We can certainly——

The CHAIRMAN. Or enforce it?

Mr. LEIBOWITZ.—encourage it. And I think some companies are in the process of migrating toward that. I think if we work together, we use our bully pulpit; and maybe if companies don't move forward quickly enough there might be a legislative approach, as well, and we want to work with you on that, if that is where this committee is going.

The CHAIRMAN. Thank you.

Senator DORGAN [presiding]. Thank you, Senator Rockefeller.

Senator Johanns.

Senator JOHANNS. Let me ask you a couple of specific questions. And I'll tell you where I'm headed on this. I hear your statement about, you know, let's put the privacy policy up, and then I can read it, and I can figure out whether I want to click on, "Yes, I agree with this," or, "I don't agree with it."

I'm coming from a different angle. Why don't we want the power of that on my side? And here are a couple of examples:

Every once in a while—and I'll bet people in the audience and listening in can relate to this—I get an e-mail from somebody advising me on the latest deal in penny stocks, "Buy this stock today." First time I got it I thought, "Well, this is easy. I'll just send an e-mail back to Joe Smith," whoever the person was, and tell him, "Please take me off your list. I don't want your e-mails anymore." So, it comes back to me, "Your e-mail is not deliverable." Why can't we require that, if I don't want to be on Joe's list to get his advice on penny stocks, I don't have to get it?

Mr. LEIBOWITZ. May I just respond to that? So, there's supposed to be an easy opt-out, under the CAN–SPAM Act, legislation that came out of this committee—Senator Dorgan was very involved in

it. And if you can't simply click on an easy opt-out mechanism, then they're in violation of CAN–SPAM. So, you can send those e-mails to me, we'll have a discussion about it, and we'll follow up, because they're not supposed to do it. And I think most legitimate companies want to have an easy opt-out mechanism. They want to be in compliance with the law.

Senator JOHANNS. Great.

Senator DORGAN. Senator Johanns, might I just point out that there is—in almost all cases, when you get that kind of e-mail, there is, way down at the end, an—generally, an "unsubscribe"——

Mr. LEIBOWITZ. Unsubscribe.

Senator DORGAN.—"icon," and so—but, if that does not exist, I think they are in violation of the law.

Mr. LEIBOWITZ. If they are in violation of the law—and, I actually went online to buy movie tickets a few weeks ago, and I have been pushing the "unsubscribe" button because I'm getting all sorts of—I wouldn't call it "spam," because it's permissible, I suppose, it's just junk corporate mail from this film-buying service. And so, not all the "unsubscribe" buttons work properly, but we're also going to work on that——

Senator JOHANNS. Yes.

Mr. LEIBOWITZ.—company, as well.

[Laughter.]

Senator JOHANNS. Well, the second question is along the same lines. And again, people relate to this. I go to my doctor, the doctor says, "You've got this condition." Quite honestly, I want that to be enormously private, maybe only share it with my wife. And so, I go on—what's the first thing you do when you get home? You go online to your favorite search engine, and you start looking up everything you can possibly look up. And you spend half the night trying to figure out, "Am I dying of cancer, or whatever it is?" Now, is there somebody out there, with that search engine company, tracing that? And next week, I start getting mailings or e-mails, or whatever, saying, you know, "You need to contact this company. They've got a product that will help with this medical condition"? Why can't I have, in my e-mail, a disclaimer that says, "Look, folks, I don't want this to be used for that purpose"?

Mr. LEIBOWITZ. Well, let me respond to that. If you're going on a large search engine, presumably they're anonymizing your data, and they're supposed to do that. And so, you do have some layer of protection. I think, when you're clicking on advertisements and you're doing other things—or you're browsing through the Internet—that's where I begin to worry about third-party cookies that track all of your wanderings in——

Senator JOHANNS. Right.

Mr. LEIBOWITZ.—cyberspace. I would say this, though. Even with respect to Google or another search engine, sometimes there's an aggregation of data that, if it became public, even though it doesn't have any, what we would call, "original personally identifiable information," could still create a pretty good profile of you.

And AOL, a few years ago, had a search engine; they released, for research purposes, a bunch of anonymized searches. And the New York Times did a very clever thing. They sort of reconstructed it, and they came up with some of the people who had done these

searches. And so, I think the concern you raise is a very legitimate one.

Again, we all understand that there are some wonderful benefits of being able to do all of the things that we need to do and want to do on the Internet, but we have to be very mindful—and we try to be, and I know the FCC does, under Chairman Genachowski—about protecting people's privacy.

Senator JOHANNS. Well, I'm out of time. But, you can kind of see where my questions are going. My point is this: I don't think this is what people are signing up for. I think it is a wonderful tool. I think you can do rather remarkable things, more things than even I would ever understand. But, I think we have an obligation here to try to deal with people's expectation of privacy. And, if I'm out there—maybe I do want to click on an advertisement, see what the best remedy for cancer is, or whatever—I don't want to be subjected, then, to some kind of analysis of my behavioral profile.

Mr. LEIBOWITZ. We absolutely agree with you, and we have a two-pronged approach to this. One is when we see a company violating a privacy policy or making a representation to consumers that they then don't live up to, we go after them. And we have brought lots of cases, well over 100 in this area. And then, we're trying to think through what the rules of the road ought to be in—for privacy protections and for clear privacy notices.

And that's what we're trying to do, sir. I think we're in general agreement.

Senator JOHANNS. Great.

Thank you, Mr. Chairman.

Senator DORGAN. Thank you.

Senator LeMieux.

STATEMENT OF HON. GEORGE S. LEMIEUX, U.S. SENATOR FROM FLORIDA

Senator LEMIEUX. Thank you, Mr. Chairman.

I know Chairman Rockefeller is not here, but I want to commend him for calling this hearing.

And I want to thank you both for the work that you're doing on this topic.

And I want to especially commend you, Chairman Leibowitz, on the common sense, practical way you're trying to work with the community through these roundtables to have the private sector, hopefully, fashion their own remedies so that it doesn't have to be done by regulation. I think that's always the best method, if it can be achieved. I mean, I think the private sector knows that, if it can't be, that Congress will step in. So, we're there as the backstop to, maybe, give you a little negotiating leverage. But, if the private sector will do that, I think that's the best, to all concerned.

And I want to speak to the issue that my colleague from Nebraska was talking about, and that is, this really all comes down to making sure the consumer knows what the disclosure issues are. And it's not a privacy statement, as you correctly pointed out, because you are not gaining rights by going through the privacy statement. It is a "disclosure of personal information" statement, and if it were titled that way, people would look at it a lot differently than if they see "privacy." And if we had some uniformity,

like I know was done with credit cards, with the box that you see, on your credit card statement, that is in bold—that this Congress passed that regulation in the past, and people on this committee, I know, worked on that—allows you to see, in clear writing, what it is, and there's some uniformity to it—I think that that is good for consumers. I also think it's good for the private sector, because, if people feel secure in their privacy, they're more likely to engage in transactions on the Internet, and are not going to feel like they cannot.

So, I commend you for that, and encourage you to go forward on that.

Mr. LEIBOWITZ. Well, we agree with you. And the notion of a box, where those rights are clearly articulated, in a way that consumers can see it, is one thing that we're certainly thinking about.

Senator LEMIEUX. And I like the affirmative check-off that you're talking about, so that it's not that—you know, people don't know what "cookies" are. And this—you know, when you see the little thing come up on your Website, you know, "enable cookies" or "disable cookies," that is not clear to folks. And the idea that, if you were shopping in a shopping center, and you were in The Gap, and the sales associate said to you, "OK, from now on, since you shopped here today, we are going to follow you around the mall and view your consumer transactions," no person would ever agree to that.

So, I understand that, in some transactions, I may want my search engine to provide me with information that will help me in my searches, but I think that that has to be a clear consumer choice. And I think that having the opt-in portion, that you mentioned, is very important about that.

Tell me what kind of complaints you're getting from consumers. Is there anything that's new to your attention? Are there new developments on the online world that we should be aware of?

Mr. LEIBOWITZ. Well, I would say this. You know, we get lots of inadequate data-security complaints, and we've brought cases, and I think we brought some of them with State AGs. We've done a lot of mortgage cases with——

Senator LEMIEUX. Right.

Mr. LEIBOWITZ.—State AGs, which is a——

Senator LEMIEUX. You've done a lot of them in Florida.

Mr. LEIBOWITZ.—terrific partnership, and a lot of work in Florida. That's exactly right. We get a lot of general privacy complaints that we go and we investigate. And we have brought a number of cases here.

One of the most interesting cases was a case involving Sears. Sears did data mining of consumers. It took a lot of their personal information, like prescription drug records. They paid consumers $10, and they said, "If you opt into our Sears Club we'll help you with your browsing." And they collected all this information—bank account information, prescription drug information, all sorts of personal information that they shouldn't have gotten from consumers. And consumers had no clear notice that they were getting it. It was multiple clicks away.

And we brought a case against Sears, and they stopped their bad practices. But, one of the most interesting things was that Sears

wasn't doing anything bad with this information, they didn't quite know what they were doing with this information. But, in and of itself, that's kind of disturbing, because here's a wonderful corporation, and they were collecting this information. They weren't giving, in our opinion, consumers adequate notice.

And again, part of the reason we partner with State AGs is because we are a tiny agency, by Washington standards. You know, we do consumer protection, we do antitrust. But, you do wonder how many other instances there are of companies collecting data and doing inappropriate things with them.

Senator LEMIEUX. Well, again, I commend you for trying to work with business on it. Coming to clear agreed-to standards is good for the business community, because it allows them to operate, and it's also good for consumers. And I know that—on the FCC side, that there are probably resources that you can use to bring to bear to help in these efforts, so—appreciate the collaboration between the two agencies.

Senator LEMIEUX. Thank you, Mr. Chairman.

Senator DORGAN. Thank you, Senator LeMieux.

Senator Thune?

STATEMENT OF HON. JOHN THUNE,
U.S. SENATOR FROM SOUTH DAKOTA

Senator THUNE. Thank you, Mr. Chairman.

Let me just ask, from a regulatory perspective—there seems to be a significant debate over how to address the collection of certain types of information. If new regulations were to be enacted, should they address the collection of different types of information in different ways? For example, how should Congress make this distinction? And, maybe to put a finer point on it, if Congress were to try to and define what constitutes "personally identifiable information," how would we go about doing that?

Mr. LEIBOWITZ. So, "personally identifiable information" includes the core traditional things. It's your name, it's your address, it's your Social Security number. But, of course, we have pretty much said—and all the commissioners, Democrat or Republican, Independent—are in agreement that "personally identifiable information," in the Information Age we live in, with these extraordinary amounts of aggregated data, is a little bit broader than that.

One thing you might focus on, if this committee moves ahead with legislation, is thinking about different rules of the road for sensitive information being collected, going back to your point. I think that's important. You always want clear notice, but maybe, in that instance, you want clear notice and some sort of opt-in, so consumers have to affirmatively opt in for use of this kind of data.

But, as you know, it's very complicated—it's easy to go after bottom feeders and malefactors and good companies that just make mistakes, when we find them. It's hard to figure out—because we all want the free content in applications that flows through the Internet—it's hard to figure out exactly what the instrument might be.

I'll just make one more point and then I'll turn it over to my colleague, Mr. Genachowski.

One promising area—and we're trying to figure out whether the technology is quite there yet—is to do a Do Not Track, through browsers. If we could have some sort of universal easy-to-use mechanism for consumers—it could be run through the FTC, or it could be run through some sort of private-sector entity—consumers could make that choice. Now, my guess is, most consumers like seeing targeted ads for most subjects. And so, you wouldn't see a huge number of people opting out. If you opt-out, you still get advertisements, they just won't be targeted. So, that's one thing we're focusing on. And we'll be back to you when we finish our report, in the fall, and tell you what our recommendations are and whether this is one viable way to proceed.

Mr. GENACHOWSKI. The one thing I'd add to that is, you know, at the FCC we focus on the on-ramps——

Senator THUNE. Right.

Mr. GENACHOWSKI.—to the Internet, and on the goal of extending broadband and its benefits everywhere. And, one of the things that's clear to us, in our work, is that the privacy issues and concerns that we're discussing here are important, not only because they're a fundamental moral issue, a fundamental individual issue, but also because, to get the benefits of broadband—the economic benefits, telehealth, education—people need to be confident that the Internet is a safe, trustworthy place. And the more people have the concerns that we're hearing today, the less likely they are to take advantage of this medium that, we've talked about in other settings, has enormous potential to generate economic growth in the United States, innovation, transform healthcare in a positive way.

So, the multiple reasons—and I heard a couple of Senators mention this— of the importance of addressing this issue is something that we see, in our work, is very important. There's a long history, at the FCC, on focusing on the on-ramps. The statute talks about telecommunications carriers, cable and satellite companies—CPNI is the phrase that we use at the FCC, with respect to ensuring that personal information that providers have is adequately protected, secured. And—as I mentioned in my opening statement, even today there's no shortage of enforcement actions that we're called upon to bring as part of the certification program that we have for providers to make sure that they are living up to the expectations, with respect to securing the personal data that, in an analogous way, is available to companies when you make a phone call, when you connect to the Internet.

And so, collaboration, here, is very important, and we work on that on a regular basis.

Mr. LEIBOWITZ. We do. And if I could just say one more thing. You know, we also collaborate on education, which is very, very important, too. And so, here's a brochure we wrote up. And Chairman Genachowski and I announced it with the Education Secretary, Arne Duncan, called Net Cetera. And it's about how parents can talk to their kids about being online. And more than 3 million of them have distributed through schools. So, education is critically important in this area.

Senator THUNE. And I'm interested in what you mentioned in your testimony today that would allow consumers to opt-out of

tracking and behavioral—at a browser level, as opposed to website-by-website. And so, as you continue to pursue that, I'd be interested in——

Mr. LEIBOWITZ. We will——

Senator THUNE.—your findings.

Mr. LEIBOWITZ. We will——

Senator THUNE. One other——

Mr. LEIBOWITZ. We'll submit——

Senator THUNE.—quick question, if I might. And it has to do with the whole issue of cloud computing networks and how that bears on this. As government data's moving to a cloud computing network, does that improve the data security of that information? And are there particular security or privacy threats that we ought to be cognizant of as government agencies make that transition?

Mr. LEIBOWITZ. Well, cloud computing, I think, can, in some instances, increase the efficiency and provide more options for businesses, including small businesses that want to store data. In terms of the data security, and in terms of the data security for government, I think it's a really important issue. We were one of the agencies that got shut down for a day, by virtue of an attack on us from a foreign country. And so, we're very, very mindful about both securing our own data, at the FTC, and trying to make sure that there's a security component added—reasonable data security or really good data security in cloud computing.

Senator THUNE. Yes.

I see my time has expired, Mr. Chairman, so thank you very much.

Senator DORGAN. Senator Thune, thank you.

STATEMENT OF HON. BYRON L. DORGAN,
U.S. SENATOR FROM NORTH DAKOTA

I want to mention that Senator Rockefeller left, as did Senator Kerry, to go for a 3 o'clock vote—cast a vote at 3 o'clock. Turns out the vote was delayed, when they got to the floor of the Senate, until 3:20. So, the vote will begin momentarily. Let me ask a few questions in their absence.

I held a couple of hearings on these issues, when I chaired a subcommittee in this committee. I chaired two hearings in 2008. And that followed a company, called NebuAd, that was described as working with certain Internet service providers to gain access to the content on their networks to provide advertisers with profiles of those providers' customers. And so, I held a couple of hearings and we began to try to think through, How do we address these issues? And it is extraordinarily complicated, there's no question about that.

It is the case that advertising supports the Internet, in large measure. And advertising, it is the case, can be very useful to customers, to those that are on the Internet searching for a pair of shoes or a wristwatch; perhaps they've searched before for these brands. And so, there are certain things that can be helpful to customers, with respect to advertising on the Internet. But, it's also the case that the Internet provides substantial access for what I call "snooping" or "tracking." And those of us who run in modern-day campaigns, those of us who've run Senate campaigns, under-

stand what the word "tracker" would mean. Modern campaigns have trackers tracking the other campaign, and recording everything. And it's not a very pleasant thing, but if you're in public life, that's the way it works. Most of the Americans who aren't in public office or in public life would find it pretty unbelievable to have a tracker tracking everything.

Let me give you an example. If someone, this afternoon, left the hearing and took the rest of the day off, and you went to Tysons Corner and stopped at Chipotle, because you're hungry and it has been a long hearing. And then you stopped that the Nordstrom's and went to ladies lingerie——

[Laughter.]

Senator DORGAN.—it's not going to—the tracker's not going to describe whether you're weird of looking for a gift for your wife.

[Laughter.]

Senator DORGAN. But, they're just going to say you stopped at ladies lingerie and purchased a little something at Nordstrom's; and then perhaps a jewelry store; and then maybe Annie's Pretzels; and then a bookstore, where you bought Rolling Stone, Better Homes and Gardens, and "How to Make a Nuclear Weapon."

[Laughter.]

Senator DORGAN. And so, someone followed you at every step of the way, just over your shoulder, making copious notes on your behavior. Anyone would find that unbelievable. They would say, "Are you kidding me? Who the hell are you, tracking me around, making notes about everything I'm doing?" And yet, that's happening, every day across this country, to people that are using the Internet. And the question is: Who's gathering it? And, how is it being used? Or, how will it be used? Those are the operative questions. And that's what brings us to this table.

Let me say, to both of you——

Julius Genachowski, you know, I think you're pulling a pretty heavy load down there, working on really important things. And I'm very supportive of what you're doing. I know there's some controversy about some of them.

And, Mr. Leibowitz, the same thing with you.

We—I think this committee relies on both of your agencies to help steer us and think through, How do we work with the industry to keep that which is good—I mean, advertising, supporting the Internet, is something all of us want to be allowed to flourish—without the kind of tracking and snooping, and particularly the danger of inappropriate use of material that has been gathered about individuals?

So, having said that as a long preamble, since the two hearings that we held on this subject, Mr. Leibowitz, again, remembering NebuAd and that they—the short explosion of anger and concern about that—What do you think we have learned, from then until now, that should guide us, or could guiding us, in, first, making a judgment, Does there—Do—Is there a need for substantial additional regulations, either passed into law by the Congress or developed by the agency? Or can there be a partnership that appropriately develops the guidelines? Would that be sufficient?

Mr. LEIBOWITZ. So, here's, it seems to me, one lesson from the brief life of NebuAd and deep packet inspection. Deep packet in-

spection is, in many ways, worse than third-party cookies, because, the notion of deep packet inspection, you have to go through an ISP. So, they get all of your information with using this type of service, or they would have if, I think, that——

Senator DORGAN. And it has to be with the concurrence of the Internet service provider. Presumably, the only reason an ISP would concur is that they—they're going to get something from it.

Mr. LEIBOWITZ. Well, that's right. That's right. I mean, it might be monetizable—I'd imagine it is—but there didn't have to be any concurrence of the consumer. And so, one thing I think that we've learned from this is there's a fair amount of corporate responsibility here, because the minute we started talking about the problems of deep packet inspection, you saw companies immediately, or pretty quickly, back off of it. I would say that.

The other lesson, it seems to me, is, we need—and just following up on that, there's a group—they have the unfortunate name The Coalition—but it's a group of a number of private companies getting together to try to come up with an easy way for consumers to opt-out of targeted ads. And it's moving along, it's very promising. More than 100 corporations, I believe, are involved in this, that have big Internet presences. So, that's a good sign. And I think that's consistent with the corporate responsibility that we sometimes see, although they're not on market yet.

And then, the other thing is that consumers need to have clear notice so they can make more informed decisions, because that's critically important as well.

As for legislation, I think it's really in the hands of the private sector. If they want to do a better job of ensuring that consumers can make clear choices and have clear notice, then I think it's in their hands to avoid legislation. And I think, if they don't, and if we don't see more progress, I think you're going to see, probably next Congress, a fair amount of interest in moving legislation forward to have more prescriptive rules.

Senator DORGAN. Do you have any recollection of how we discovered the issue of NebuAd?

Mr. LEIBOWITZ. I read about it after a committee hearing, I believe. But——

Senator DORGAN. But——

Mr. LEIBOWITZ. Or——

Senator DORGAN.—we didn't have——

Mr. LEIBOWITZ.—right before that. I think—go ahead.

Senator DORGAN. Well, we didn't have a hearing, I think, because of original discovery. I mean, my recollection of that was, somebody did an enterprising piece of reporting——

Mr. LEIBOWITZ. Maybe it was in the paper.

Senator DORGAN. And——

Mr. LEIBOWITZ. Yes.

Senator DORGAN. And the result was, people saying, "Oh my God. I had no idea this was going on." Is there any assurance that—although NebuAd is not around, I mean, do we know whether it's happening now?

Mr. LEIBOWITZ. I certainly think, based on—even when we're not doing investigations, we have cable companies and telephone companies in, at least to talk to them. We actually don't have jurisdic-

tion over telephone companies for enforcement actions. We'd like to see the common carrier—and you've been a leader on that—common carrier exemption repealed. But, I think we would know about it. I would like to think that, consistent with the corporate responsibility we like to see, that they would come and tell us, and tell Chairman Genachowski what they're interested in and what they're doing.

Mr. GENACHOWSKI. I think the one thing that I'd add to that—and I agree with what Chairman Leibowitz is saying—what that history underscores is the importance of real transparency and information to consumers. Anytime it's a story that, "Well, when consumers found out about it, they rebelled," that tells us things that are both good and bad. It tells us that, with adequate information, notice, real choice, there's an increasing chance that the market can work and that companies will be moved by the—an informed market to adopt policies that work.

The other thing that I think it underscores is that the—with the technology changing as rapidly as it does, the lessons that I think we should pull out of experiences like that go to core principles and strategies that will work, regardless of how technology evolves and different opportunities that may exist to benefit from personal information. And so, a real focus on transparency, meaningful consumer choice, the kinds of ideas, around boxes, or otherwise. I have personal—as Chairman Leibowitz knows—personal experience with the credit card box when I was a staffer on the Hill 20 years ago. And I think it's a—the core idea of working to make sure that consumers have information, in a way that makes sense to them, that's actionable, it's an idea that brings together the fundamental principles of consumer choice and empowerment with a market-oriented approach that can help us get the benefits from broadband and the Internet, new technologies that we want.

Senator DORGAN. Thank you very much.

Senator Thune, did you wish to inquire——

Senator THUNE. Yes.

Senator DORGAN.—further?

Senator THUNE. Very quickly, if I might, Mr. Chairman.

Let me ask you both whether the FTC or the FCC should be the lead agency when it comes to enforcing online privacy policies. And if you had a National Broadband Plan that is fully implemented, would there be duplication of online privacy regulations between the two agencies?

Mr. GENACHOWSKI. Well, as with so many other areas, it's important that we work together. Our agencies have different kinds of expertise. We've, historically, focused on the networks. We have technological expertise; the networks, whether they're wired and wireless. Our jurisdiction is different from that of the FTC, even where they overlap.

And so, to me, continued collaboration in this area, with respect to the expertise that each of our agencies, and the kinds of enforcement tools that we have, is very important. I think it's important, as we've Net Cetera and other things—where we're working on goals like consumer education, I think it's important—and we've talked about this with each other—to do this in a coordinated way and not to—you know, to agree on a single way to inform con-

sumers, make sure that consumers are informed. One of the risks is, consumers get different information from different sources, and they're even more confused.

Mr. LEIBOWITZ. Yes, and I agree with Chairman Genachowski. We have complementary areas of expertise. I don't think anyone has ever accused us of piling on anyway. I mean, we're an enforcement agency. You're more of a regulatory agency. We have a policy component, too. And so, I think we want to work on this together.

We bring a lot of privacy cases, but, in the broadband context, I think it's important that we work together and we think about all of these issues with this committee.

Senator THUNE. Right.

Mr. GENACHOWSKI. And I would add, as I said in my opening statement, one of the things that the Broadband Plan pointed out, in addition to the point that having consumer confidence around privacy is actually important for economic growth relating to broadband, there is uncertainty in the landscape. You know, in the Communications Act, it speaks about telecommunications areas—carriers, cable, satellite—ad the traditional work that the FCC has done—to make sure that your personal information, when a telephone company has it or a cable company has it, is protected, needs to be clarified for the new technologies that provide communications access service to consumers.

So, it is an area that we look forward to working on with the Committee and with each other. But, it is important that we look at all of the laws and regulations, and make sure that they actually make sense, given the way that consumers today access communications services.

Senator THUNE. One last question, very quickly, and this would be to Chairman Leibowitz. In 2009, the FTC released a set of voluntary principles that were to be used by Web advertisers, when it comes to this whole issue of protecting consumers and aiding the industry in self-regulation. How has the industry reacted to those guidelines?

Mr. LEIBOWITZ. I think they've liked them. I mean, we had all the stakeholders together in drafting them. Those guidelines were things like, if you change your privacy policy materially, you have to give consumers a clear opt-in, because you already have their information under a different policy if you said, "We're not selling the information." But, if you change your mind, as a company, and say, "We will," you have to get a clear authorization from consumers.

So, I think it's worked out pretty well. And then as Chairman Genachowski pointed out, and as you pointed out—it's a very dynamic industry here. And so, in our next series of workshops we've done about privacy, we've also brought together all stakeholders. I think—and we're an agency that doesn't have much rulemaking authority—if you want to move forward on protecting consumers' privacy, you need to bring all the stakeholders along with you, maybe prod them a little bit more than they might like to be, and push them a little bit. But, that's the best approach. And so, I'd like to think that when we release our next guidance in the fall—or, our report—that we'll continue to have buy-in from both consumer groups and the business community and everyone else, and this committee, too.

Senator THUNE. I've got one I'll submit for the record, Mr. Chairman, on——

Senator DORGAN. All right.

Senator THUNE.—on peer-to-peer software exchanging programs, which I'd be interested in getting your——

Senator DORGAN. Right.

Senator THUNE.—answer to.

Senator DORGAN. Let me say to you that I think—you know, with respect to Senator Johanns' question, I think that what we have required with respect to "unsubscribe" is simple and pretty easy to understand. I mean, it—you go to these sites, and you buy something someplace, and they begin pushing these e-mails at you, or these advertisements, and you just go down to the end of it, and says, "Unsubscribe." Generally, it's in color or something, and fairly large, and it's just one sentence, "If you wish to unsubscribe, punch this." I think that has been really successful. I'm wondering whether there—and part of it's because it is simple. Is there a companion approach that we could use to dramatically simplify the issue of how this particular Internet site is going to use your information?

Because, frankly, my guess is neither of you—maybe I shouldn't guess. I was going to say "I'd bet," and I wouldn't want to bet, either.

[Laughter.]

Senator DORGAN. But, I'll bet neither of you read the full privacy statement on a site.

[Laughter.]

Senator DORGAN. I'm just guessing you don't do that, because——

Mr. LEIBOWITZ. Chairman Genachowski's very substantive. It's——

[Laughter.]

Senator DORGAN. Yes, but you got to be substantive for a long, long time to read through that. And, you know, in most cases, it's long statements. And so, it'd be nice if we could find a way to also improve in that area, and simplify it, so that if I'm going to a site, as a consumer, I know, pretty simply, what that site will or won't—or what it says it will or won't do with my information.

I know the site—if I'm buying a pair of shoes at a department store online, I know that particular department store is going to have my information about—I buy shoes, I buy 9D, I like Loafers. You know, they're going to have that, and I understand that, as a consumer. So will a brick-and-mortar retailer have that in their records. So, I understand that. The question—well, the more important question is, What will that retailer do with the aggregated information? And it doesn't—it's not easy to discern that, always.

Mr. LEIBOWITZ. Let me just respond to that. And the "unsubscribe" box is a great example of this committee and the Commission working together to create something that we would call "privacy by design," that really works. It's clear. It's often purple—or at the bottom, in purple or red—that you can go down, and you can unsubscribe. And it's pretty uniform where it is. I think that's a result of our rulemakings, pursuant to your direction to us to do a rule on this in CAN–SPAM. And that's the kind of thing we're looking at. It's just ways to bake in easy, clear privacy poli-

cies that consumers can understand. It's also the reason why we've been gravitating toward, if the technology is there, the notion of a clear way to opt-out of behavioral targeting through a single entity that might use the browsers, because it's easy to understand. Consumers don't read privacy policies, and they don't have a lot of time, so you want to give them some clear options, up front.

Senator DORGAN. Yes.

Mr. GENACHOWSKI. I agree with that completely. And the other—the only other point I'd add is that technology provides, every day, new ways to answer that challenge, to develop ways to put in front of consumers, at the right time, information that's actionable. And so, 2 years before you held those hearings and worked on the "unsubscribe" button, people probably wouldn't have been able to imagine that you could actually have an "unsubscribe" button, in the e-mail, that you could press and it would be very simple. When we were working on credit card information, 20 years ago, I remember, we spent a lot of time thinking about, "Well, even if there is a box, how do we get it in front of consumers in a way that actually informs their decision?" The same technology that creates these problems also provides new ways to solve it.

I think that one of the things that this hearing does, that we have both tried to do, is spur industry to use their technology expertise to help develop answers that empower consumers in a meaningful way. So, it's an important challenge, and it's one we both take up.

Senator DORGAN. All right.

In order that I don't miss this vote, I'm going to—and I think the Chairman will be here momentarily. Let me ask that the Committee stand in recess for 5 minutes.

[Recess.]

The CHAIRMAN [presiding]. People are obviously on their way back. And I apologize for interrupting the sacred protocol of the Senate Commerce Committee, but I do so because there's a very interesting witness in front of us, and I didn't quite finish.

This question of small print haunts us on this committee. We run into it on pop-ups. We run into it on health insurance. We run—you know, mortgage fraud, "We can settle your debts, just send us $10." And people call up, and the company doesn't exist, but they go on paying. I mean, it's just everywhere. And it's always brought forward and allowed—given freedom by something called small print.

I want to know, from your point of view, if you think it's a deceptive—small print is deceptive inherently or if it's deceptive in cases of specific uses. And how on earth can either you or the user tell the difference?

Mr. LEIBOWITZ. So, I would say this—and I believe the Commission has had small-print issues going back to even before the Internet. If, in small print, you have material terms, important terms to the consumers, and they're clicks away, where the consumers can't possibly find them, or a reasonable consumer couldn't find them, they're inherently deceptive or unfair. And we are going to go after people for doing that.

And then, just thinking through, in terms of the architecture of where we would like to see companies go and what we're thinking

about in our report, is to have a kind of a small box. We're not quite there yet, but the idea of a small box with the material terms in them that the consumers have to see, so that you can't get away with burying things in the fine print. And we had one case——

The CHAIRMAN. It's not necessarily large, but it's surrounded by bright red?

Mr. LEIBOWITZ. In a way that a reasonable consumer—someone who's on the Internet all the time, someone who's a coal miner from West Virginia who goes on the Internet from time to time, will understand the meaning of, and they won't be selling their soul for all eternity——

The CHAIRMAN. Yes.

Mr. LEIBOWITZ.—for failure to opt out.

The CHAIRMAN. Yes. That's—well, that was dramatic.

Do—isn't there a point at which people simply fail to be able to read, physically, small print?

Mr. LEIBOWITZ. Yes.

The CHAIRMAN. At a certain age?

Mr. LEIBOWITZ. Well, I think that there's a reason why in contracts, some clauses are buried in the fine print. It's because people want them buried there. Now, this is not the practice of the best companies, but it is certainly the practice of the worst companies.

We had one case involving a company that acknowledged, in its pleadings—in its court papers, that it was responsible for 6 billion popup ads to consumers—6 billion popup ads. I don't think consumers understood—and there was some sort of warning, multiple clicks away, but I don't think a single consumer consented to downloading software that was going to serve them pop-up ads, you know, until we shut the company down.

So, we want to work with you on this. You missed Senator Dorgan, because he was leaving as you were coming, but he made the same point about the "unsubscribe" notice at the bottom of a lot of e-mails. You know, one of the things we want to try to do is to have this stuff baked into the interactions that companies have with consumers in a way that consumers can clearly understand it. And we're hoping companies will do this themselves, but, if they don't do it themselves, we'll be working with you on the Committee to try to craft legislation that will move forward.

The CHAIRMAN. When you ask large and successful companies, who are riding the waves of success and popular demand, to do something on a voluntary basis, which they really don't want to do, do they generally not do it?

Mr. LEIBOWITZ. I think it's different responses by different companies. I think a lot of companies recognize that their brand is enhanced if they're not doing things that are, if not deceptive, then in a gray area. For some companies, you have to push and prod to get them to do the right thing. A lot of them will do it—and then some companies just don't.

We brought a major case against Sears for data mining without giving consumers notice and consent. And they weren't doing anything bad with the information, they just were taking it without the permission of consumers, and it included prescription drug information and other personal information.

And so, it really depends, but I think having these hearings is enormously important in moving companies forward toward doing the right thing.

The CHAIRMAN. When you were here, before we all left, you referred to the opt-in/opt-out question, and you seemed to come down on the side of opt-in.

Mr. LEIBOWITZ. I——

The CHAIRMAN. Tell me what you—what—how you discern the one from the other.

Mr. LEIBOWITZ. So, the most important thing is——

The CHAIRMAN. I mean——

Mr. LEIBOWITZ.—clear notice——

The CHAIRMAN.—I know what it means.

Mr. LEIBOWITZ.—to consumers.

The CHAIRMAN. But, I mean——

Mr. LEIBOWITZ. Right.

The CHAIRMAN.—how do you——

Mr. LEIBOWITZ. The most important thing is clear notice to consumers. From my perspective—and not everyone on the Commission shares this view—I think it's probably a majority, but I'm not entirely certain—I think opt-in protects consumers' privacy better than opt-out under most circumstances. I don't think it undermines a company's ability to get information that it needs to advertise back to consumers. And so, that's my preference.

And then, I think the entire Commission believes that, when you're dealing with sensitive information, or changing an existing privacy policy, that has to be opt-in. You have to give consumers clear notice that you're changing your privacy policy and that they're opting into it.

The CHAIRMAN. And your argument there would be, because if you wait for the opt-out, that means they've already been had- and haven't had a chance to—they can't undo——

Mr. LEIBOWITZ. Well, I——

The CHAIRMAN.—what they've done.

Mr. LEIBOWITZ. Right. I mean, speaking hypothetically, not with respect to a particular instance, the argument is this: If a company says, "I am going to not share your information with any other companies or any of our affiliates," and then they decide to change their policy, most consumers won't read that policy, because why would they? And so, you have to give them a clear ability to opt in to your new policy.

And, with respect to sensitive information, like medical information or bank records or personal medical information, the privacy level is so important, because this is the kind of information you don't want circulating around on the Internet, that you want an additional degree of privacy protection. And there, I think the whole Commission agrees that this should be an opt-in approach.

The CHAIRMAN. One more question.

Mr. LEIBOWITZ. Yes, sir.

The CHAIRMAN. And I apologize. What if the privacy policy discloses that it will sell a consumer data to a third party, or parties, who can use that information for increasing insurance rates or creating profiles for potential employers? Is that fair, if the consumer never reads the policy?

Mr. LEIBOWITZ. It would be something we would want to take a very close look at. And if your staff has any instances of policies like that, please send them our way.

The CHAIRMAN. How do you describe, then, what the—and I'm not on the side of the question I'm asking. I want to make——

Mr. LEIBOWITZ. Right.

The CHAIRMAN.—that clear. People often say, "Well parents should do this. They should set the remote so kids can't watch such-and-such on TV when they're double working, stressed, and all kinds of things." But, second, the responsibility of the consumer, that's a little bit of the argument I heard last night at the dinner table. And I didn't like it.

In other words, if people have a responsibility—they're entering into a situation—they know that, they know it's a complex world—and therefore they should take all of that very seriously. I think that's asking the impossible of the average, non-elite user.

Mr. LEIBOWITZ. Well, I agree with that. But, I will say this: We're not at the level yet where every company even gives consumers clear notice so that they can make clear choices. Most of the cases we've brought involve instances where, going back to your first point, the disclosures or the use of the information was in the fine print that was designed to ensure that consumers really wouldn't find it.

And so, I think the best companies want to make these things clear. I think we need to ensure that other companies move to that level.

The CHAIRMAN. Well, thank you, Chairman Leibowitz.

Mr. LEIBOWITZ. Thank you, Chairman Rockefeller.

The CHAIRMAN. All right.

Mr. LEIBOWITZ. All right.

The CHAIRMAN. Thank you, sir.

Our second panel—maybe this is outrageous on my part, to call them, but I'm going to—is Dr. Guy Tribble, who's Vice President, Software Technology, Apple; Mr. Bret Taylor, Chief Technology Officer, Facebook; Dr. Alma Whitten, Privacy Engineering Lead, Google; Mr. Jim Harper, Director of Information Policy Studies at The Cato Institute; Ms. Dorothy Attwood, Senior Vice President of Public Policy, and Chief Privacy Officer, AT&T; and Professor Joseph Turow, Annenberg School of Communication, who has been before us many times. If you can possibly find seats——

[Laughter.]

The CHAIRMAN. And make sure they have plenty of water. This is a hydration-type day—not "hearing," day.

Let me just go in the order of the way it appears before me here, Panel 2.

Dr. Tribble, of Apple.

STATEMENT OF DR. GUY "BUD" TRIBBLE, VICE PRESIDENT, SOFTWARE TECHNOLOGY, APPLE INC.

Dr. TRIBBLE. Good afternoon, Chairman Rockefeller, and members of the Committee.

My name is Bud Tribble. I'm Vice President for Software Technology at Apple. Thank you for inviting me today to testify about Apple's approach to consumer privacy.

Apple shares your concerns about privacy, and we remain deeply committed to protecting the privacy of our customers through a comprehensive approach implemented throughout the company. We're committed to providing our customers with clear notice, choice, and control over their information.

For instance, as part of our location-based service, we provide our customers with easy-to-use tools that let them control the collection and use of location data on all our devices. I'd also like to point out, considering the opening remarks, that Apple does not share our customers' private data, or sell our customers' private data, to third parties for their marketing purposes.

As we have provided the Committee an explanation of our privacy practices in our written testimony, I'd like to use my limited time this afternoon to emphasize a few points about our innovative and easy-to-use controls which let customers manage how applications use and collect their location data. We believe that, in addition to a published privacy policy, it's very helpful to have privacy features actually built and designed into the device's user interface, and would like to describe some of Apple's innovations and practices in this area.

First, Apple does not allow any application to receive device location information without the user's permission. Apple's rule with respect to the use of location data by an application is simple. If an app, whether a third-party app or an Apple app, wants to use the device's location it must get the consumer's explicit consent. This consent is obtained through a simple popup dialogue box. The dialogue box is mandatory. Neither the third-party app nor Apple apps are permitted to override this notification. Only after the user has authorized it will the app be allowed to use device location data.

So, how does this work? Say you're in an unfamiliar neighborhood looking for a nearby restaurant. You launch a third-party app, that you've just installed, that can provide you with that information, but first it needs to know where you are in order to help. After it launches, before the app receives any device location information, the software prompts you that the app would like to use your current location. And it presents two options: "Don't allow," or "OK." With your OK, your device sends encrypted anonymous location data to Apple, which in turn provides the app with the coordinates it needs to determine which restaurants are nearby.

In this example, information about the device's actual location is only transmitted to the third-party application after the customer expressly consents. Equally important, Apple has built a Master Location Services switch into our iOS mobile operating system, which makes it extremely easy to opt out, entirely, of location-based services. The user simply switches the location services to "Off," in the settings screen. When this switch is turned off, all location-sharing is turned off.

With our iOS4 released in June, the iPhone 4, iPhone 3GS, and iPhone 3G, as well as our more recent iPod touch devices, now display an arrow icon in the status bar at the top of the screen, near the battery indicator, as a reminder to the user that location data is being shared with apps. In addition, with iOS4, customers are able to view a list of every app that they have authorized to access

their location information. And this innovation even uses that arrow icon to indicate which apps have used your location-based data within the past 24 hours, and allows customers to easily turn location-sharing off and on individually for each app, with a simple tap.

I should point out, as well, that not using these location services does not impact the nonlocation-based functionality of the iPhone.

With more than 100 million iOS devices sold to date, and more than 3 billion apps downloaded from our apps store, millions of people around the world have experienced this process. We believe it's a simple and direct way to keep customers informed and in control of their location-based data.

In closing, let me state again that Apple is strongly committed to giving our customers clear notice, choice, and control over their information. And we believe that our products do this in a simple and elegant way. We share the Committee's concerns about the collection and misuse of all customer data, particularly location data, and appreciate this opportunity to explain our approach this afternoon. I'll be happy to answer any questions you may have.

[The prepared statement of Dr. Tribble follows:]

PREPARED STATEMENT OF DR. GUY "BUD" TRIBBLE, VICE PRESIDENT, SOFTWARE TECHNOLOGY, APPLE INC.

Good afternoon Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee. My name is Bud Tribble, and I am Vice President for Software Technology for Apple Inc. Thank you for inviting me today to testify about Apple's approach to consumer privacy.

Apple's Customer Privacy Commitment

First, Apple shares your concerns about privacy, and we remain deeply committed to protecting the privacy of our customers through a comprehensive approach implemented throughout the company. At Apple, we are committed to providing our customers with clear notice, choice and control over their information. To accomplish this goal, we have innovated easy to use tools that allow our consumers to control the collection and use of location-based services data on all of our devices. Finally, we do not share personally identifiable information with third parties for their marketing purposes.

In order to explain our comprehensive approach to privacy, I have divided my testimony in to three sections: (1) Apple's Privacy Policy; (2) Location-Based Services; and (3) Third-Party Applications.

1. Apple's Privacy Policy

Apple has a single Customer Privacy Policy (the "Policy") that applies across all Apple businesses and products, including the iTunes Store and App Store.[1] The Policy, written in easy-to-read language, details what information Apple collects and how Apple and its partners and licensees may use the information. The Policy is available from a link on every page of Apple's website.[2]

As you may be aware, Apple updated its Policy just this past month, to add, among other changes discussed below, the following provision regarding location-based information:

> To provide location-based services on Apple products, Apple and our partners and licensees may collect, use, and share precise location data, including the real-time geographic location of your Apple computer or device. This location data is collected anonymously in a form that does not personally identify you and is used by Apple and our partners and licensees to provide and improve location-based products and services. For example, we may share geographic location with application providers when you opt in to their location services.

[1] As used in the policy and in this letter, "Apple," refers to Apple Inc. and affiliated companies.

[2] The links take customers to *http://www.apple.com/legal/privacy*, which may also be accessed by customers directly.

> Some location-based services offered by Apple, such as the MobileMe "Find My iPhone" feature, require your personal information for the feature to work.

This provision incorporated similar language regarding location-based information that appears in Apple End User Software License Agreements ("SLAs") for products that provide location-based services. For example, the current iPhone 3GS SLA, last updated in May 2009, states:

> Apple and its partners and licensees may provide certain services through your iPhone that rely upon location information. To provide these services, where available, Apple and its partners and licensees may transmit, collect, maintain, process and use your location data, including the real-time geographic location of your iPhone, and location search queries. The location data collected by Apple is collected in a form that does not personally identify you and may be used by Apple and its partners and licensees to provide location-based products and services. By using any location-based services on your iPhone, you agree and consent to Apple's and its partners' and licensees' transmission, collection, maintenance, processing and use of your location data to provide such products and services. You may withdraw this consent at any time by not using the location-based features or by turning off the Location Services setting on your iPhone. Not using these location features will not impact the non location-based functionality of your iPhone. When using third party applications or services on the iPhone that use or provide location data, you are subject to and should review such third party's terms and privacy policy on use of location data by such third party applications or services.

Similar provisions regarding location-based information appear in the iPhone 4, iPad, iPod Touch, Mac OS X, and Safari 5 SLAs.

The Policy identifies dedicated e-mail addresses for privacy-related inquiries and comments. Apple monitors these e-mail addresses and responds to appropriate inquiries in a timely manner. Customers may also address privacy concerns to TRUSTe, Apple's third-party privacy monitor. A link to TRUSTe is displayed within the Policy.

June 2010 Policy Update

In the past 3 years, Apple revised its Policy three times: June 29, 2007, early February 2008, and June 21, 2010.

The June 29, 2007 update advised customers about the necessary exchange of information between Apple and the relevant cellular carrier when an iPhone is activated. Apple also added a provision stating that it does "not knowingly collect personal information from children." The provision explained that if such information was collected inadvertently, Apple would attempt to delete it "as soon as possible."

The February 2008 Policy update revised language regarding Apple's use of "pixel tags." Pixel tags are tiny graphic images used to determine what parts of Apple's website customers visited or to measure the effectiveness of searches performed on Apple's website. The revised language stated that: "[Apple] may use this information to reduce or eliminate messages sent to a customer."

On June 21, 2010, Apple updated the Policy to incorporate the language regarding location-based services from Apple SLAs, as discussed above. Apple also added provisions regarding new Apple services, such as Apple's MobileMe "Find My iPhone" feature and the iAd network. Apple made the following, additional material changes to the Policy:

- Revised provisions regarding: (i) what information Apple collects from customers and how Apple and its partners and licensees may use the information, (ii) the use of "Cookies and Other Technologies," (iii) the safeguards in place to prevent the collection of personal information from children, and (iv) the collection and use of information from international customers; and
- Added provisions: (i) advising customers to review the privacy practices of third-party application providers and (ii) cautioning customers about posting personal information on an Apple forum, chat room, or social networking service.

As noted above, customers may access the updated Policy from every page on Apple's website. The updated Policy also was placed where Apple believed the largest number of customers would see it: the iTunes Store. Following the update, every customer logging onto the iTunes Store is prompted to review the iTunes Store Terms and Conditions. For customers with existing iTunes accounts, the webpage states:

> iTunes Store Terms and Conditions have changed. Apple's Privacy Policy
>
> The changes we have made to the terms and conditions include the following:

> Apple's Privacy Policy has changed in material ways. Please visit *www.apple.com/legal/privacy* or view below.

Customers are asked to click an unchecked agreement box stating: "I have read and agree to the iTunes Terms and Conditions and Apple's Privacy Policy." Customers who do not agree to the Terms and Conditions and the Policy will not be able to use the iTunes Store (*e.g.,* will not be able to make purchases on the iTunes Store or the App Store), but they may continue to use iTunes software.

Customers attempting to open a new iTunes account are directed to a webpage titled: "iTunes Store Terms & Conditions and Apple's Privacy Policy." They are asked to click the same unchecked agreement box stating: "I have read and agree to the iTunes Terms and Conditions and Apple's Privacy Policy." Customers who do not accept the Terms and Conditions and the Policy will not be able to open an iTunes account but may still activate and use their devices.

2. Location-based Services

In response to increasing customer demand, Apple began to provide location-based services in January 2008. These services enable applications that allow customers to perform a wide variety of useful tasks such as getting directions to a particular address from their current location, locating their friends or letting their friends know where they are, or identifying nearby restaurants or stores.

Apple offers location-based services on the iPhone 3G, iPhone 3GS, iPhone 4, iPad Wi-Fi + 3G, and, to a more limited extent, older models of the iPhone, the iPad Wi-Fi, iPod touch, Mac computers running Snow Leopard,[3] and Windows or Mac computers running Safari 5.[4]

Although Apple's customers value these services and may use them on a daily basis, Apple recognizes that some customers may not be interested in such services at all times. As discussed below, Apple provides its customers with tools to control if and when location-based information is collected from them.

A. Privacy Features

Apple has always provided its customers with the ability to control the location-based service capabilities of their devices. In fact, Apple now provides customers even greater control over such capabilities for devices running the current version of Apple's mobile operating system—iOS 4.[5]

First, customers have always had the ability to turn "Off" all location-based service capabilities with a single "On/Off" toggle switch. For mobile devices, the toggle switch is in the "General" menu under "Settings." For Mac computers running Snow Leopard, the toggle switch is in the "Security" menu under "System Preferences." And for Safari 5, the toggle switch is in the "Security" menu in Safari "Preferences." If customers toggle the switch to "Off," they may not use location-based services, and no location-based information will be collected.

Second, Apple has always required express customer consent when any application or website requests location-based information for the first time. When an application or website requests the information, a dialogue box appears stating: "[Application/Website] would like to use your current location." The customer is asked: "Don't Allow" or "OK." If the customer clicks on "Don't Allow," no location-based information will be collected or transmitted. This dialogue box is mandatory—neither Apple nor third-parties are permitted to override the notification.

Third, iOS 4 permits customers to identify individual applications that may not access location-based information, even though the global location-based service capabilities setting may be toggled to "On." The "General" menu under "Settings" provides an "On/Off" toggle switch for each application. When the switch for a particular application is toggled to "Off," no location-based information will be collected or transmitted for that application. And even if the switch for an application is toggled to "On," the "Don't Allow/OK" dialogue box will request confirmation from the customer the first time that application requests location-based information. Customers can change their individual application settings at any time.

---

[3] All of Apple's Mac computers, *e.g.,* MacBook, MacBook Pro, MacBook Air, iMac, Mac mini, and Mac Pro, run on its proprietary Mac OS operating system. Apple released the current version, Mac OS X version 10.6, known as "Snow Leopard," on August 28, 2009.

[4] Safari is Apple's proprietary Internet browser. Apple released the current version of Safari version 5, on June 7, 2010.

[5] All of Apple's mobile devices run on its proprietary mobile operating system. Apple released the current version, iOS 4, on June 21, 2010. Currently, iOS 4 may be run on the iPhone 3G, iPhone 3GS, iPhone 4, and iPod touch. The iPad Wi-Fi + 3G, iPad Wi-Fi, and older models of the iPhone run on prior versions of Apple's mobile operating system, referred to as iPhone OS. Apple has released iPhone OS versions 1.0 through 3.2.

Finally, an arrow icon (➢) alerts iOS 4 users that an application is using or has recently used location-based information. This icon will appear real-time for currently running applications and next to the "On/Off" toggle switch for any application that has used location-based information in the past twenty-four hours.

B. Location-Based Information

To provide the high quality products and services that its customers demand, Apple must have access to comprehensive location-based information. For devices running the iPhone OS versions 1.1.3 to 3.1, Apple relied on (and still relies on) databases maintained by Google and Skyhook Wireless ("Skyhook") to provide location-based services. Beginning with the iPhone OS version 3.2 released in April 2010, Apple relies on its own databases to provide location-based services and for diagnostic purposes. These databases must be updated continuously to account for, among other things, the ever-changing physical landscape, more innovative uses of mobile technology, and the increasing number of Apple's customers. Apple always has taken great care to protect the privacy of its customers.

1. Cell Tower and Wi-Fi Information

a. Collections and Transmissions from Apple Mobile Devices

To provide location-based services, Apple must be able to determine quickly and precisely where a device is located. To do this, Apple maintains a secure database containing information regarding known locations of cell towers and Wi-Fi access points. The information is stored in a database accessible only by Apple and does not reveal personal information about any customer.

Information about nearby cell towers and Wi-Fi access points is collected and sent to Apple with the GPS coordinates of the device, if available: (1) when a customer requests current location information and (2) automatically, in some cases, to update and maintain databases with known location information. In both cases, the device collects the following anonymous information:

- *Cell Tower Information:* Apple collects information about nearby cell towers, such as the location of the tower(s), Cell IDs, and data about the strength of the signal transmitted from the towers. A Cell ID refers to the unique number assigned by a cellular provider to a cell, a defined geographic area covered by a cell tower in a mobile network. Cell IDs do not provide any personal information about mobile phone users located in the cell. Location, Cell ID, and signal strength information is available to anyone with certain commercially available software.
- *Wi-Fi Access Point Information:* Apple collects information about nearby Wi-Fi access points, such as the location of the access point(s), Media Access Control (MAC) addresses, and data about the strength and speed of the signal transmitted by the access point(s). A MAC address (a term that does not refer to Apple products) is a unique number assigned by a manufacturer to a network adapter or network interface card ("NIC"). The address provides the means by which a computer or mobile device is able to connect to the Internet. MAC addresses do not provide any personal information about the owner of the network adapter or NIC. Anyone with a wireless network adapter or NIC can identify the MAC address of a Wi-Fi access point. Apple does not collect the user-assigned name of the Wi-Fi access point (known as the "SSID," or service set identifier) or data being transmitted over the Wi-Fi network (known as "payload data").

First, when a customer requests current location information, the device encrypts and transmits Cell Tower and Wi-Fi Access Point Information and the device's GPS coordinates (if available) over a secure Wi-Fi Internet connection to Apple.[6] For requests transmitted from devices running the iPhone OS version 3.2 or iOS 4, Apple will retrieve known locations for nearby cell towers and Wi-Fi access points from its proprietary database and transmit the information back to the device. For requests transmitted from devices running prior versions of the iPhone OS, Apple transmits—anonymously—the Cell Tower Information to Google[7] and Wi-Fi Access Point Information to Skyhook. These providers return to Apple known locations of nearby cell towers and Wi-Fi access points, which Apple transmits back to the de-

[6] Requests sent from devices running older versions of the iPhone OS also include a random identification number that is generated by the device every ninety days. This number cannot be used to identify any particular user or device.

[7] For GPS-enabled devices running prior versions of the iPhone OS, Apple also sends the device's GPS coordinates, if available, anonymously to Google so that Google can update its database of known locations.

vice. The device uses the information, along with GPS coordinates (if available), to determine its actual location. Information about the device's actual location is not transmitted to Apple, Skyhook, or Google. Nor is it transmitted to any third-party application provider, unless the customer expressly consents.

Second, to help Apple update and maintain its database with known location information, Apple may also collect and transmit Cell Tower and Wi-Fi Access Point Information automatically. With one exception,[8] Apple automatically collects this information only: (1) if the device's location-based service capabilities are toggled to "On" and (2) the customer uses an application requiring location-based information. If both conditions are met, the device intermittently and anonymously collects Cell Tower and Wi-Fi Access Point Information from the cell towers and Wi-Fi access points that it can "see," along with the device's GPS coordinates, if available. This information is batched and then encrypted and transmitted to Apple over a Wi-Fi Internet connection every twelve hours (or later if the device does not have Wi-Fi Internet access at that time).

b. Collections and Transmissions from Computers Running Snow Leopard and/or Safari 5

Apple collects Wi-Fi Access Point Information when a Mac computer running Snow Leopard makes a location-based request—for example, if a customer asks for the current time zone to be set automatically. The information is collected anonymously and is stored in a database accessible only by Apple. Snow Leopard users can prevent the collection of this information by toggling the "Location Services" setting to "Off" in the "Security" menu under "System Preferences."

Apple also provides location-based services in Safari 5. When a customer is using Safari 5 and runs an Internet application that requests location-based information (*e.g.,* Google Maps), a dialog box will appears stating: "[Website name] would like to use your computer location." If the customer selects "Don't Allow," no location-based information is transmitted by the computer. If the customer selects "OK," Wi-Fi Access Point Information is transmitted to Apple with the request, so that Apple can return information about the computer's location. Apple does not store any Wi-Fi Access Point Information sent with requests from Safari 5.

2. Diagnostic Information

To evaluate and improve the performance of its mobile hardware and operating system, Apple collects diagnostic information from randomly-selected iPhones and analyzes the collected information. For example, when an iPhone customer makes a call, Apple may determine the device's approximate location at the beginning and end of the call to analyze whether a problem like dropped calls is occurring on the same device repeatedly or by multiple devices in the same area. Apple determines the approximate location by collecting information about nearby cell towers and Wi-Fi access points and comparing that with known cell tower and Wi-Fi access point locations in Apple's database. Apple may also collect signal strength information to identify locations with reception issues.

Before any diagnostic information is collected, the customer must provide express consent to Apple. If the customer consents, the information is sent to Apple over a secure connection. The information is sent anonymously and cannot be associated with a particular user or device. The diagnostic information is stored in a database accessible only by Apple. If the customer does not consent, Apple will not collect any diagnostic information.

3. GPS Information

The iPhone 3G, iPhone 3GS, iPhone 4, and iPad Wi-Fi + 3G are equipped with GPS chips. A GPS chip attempts to determine a device's location by analyzing how long it takes for satellite signals to reach the device. Through this analysis, the GPS chip can identify the device's latitude/longitude coordinates, altitude, speed and direction of travel, and the current date and time where the device is located ("GPS Information").

Apple collects GPS Information from mobile devices running the iPhone OS 3.2 or iOS 4. GPS Information may be used, for example, to analyze traffic patterns and

---

[8] For GPS-enabled devices with location-based service capabilities toggled to "On," Apple automatically collects Wi-Fi Access Point Information and GPS coordinates when a device is searching for a cellular network, such as when the device is first turned on or trying to re-establish a dropped connection. The device searches for nearby Wi-Fi access points for approximately thirty seconds. The device collects anonymous Wi-Fi Access Point Information for those that it can "see." This information and the GPS coordinates are stored (or "batched") on the device and added to the information sent to Apple. None of the information transmitted to Apple is associated with a particular user or device.

density in various areas. With one exception,[9] Apple collects GPS Information only if: (1) the location-based service capabilities of the device are toggled to "On" and (2) the customer uses an application requiring GPS capabilities. The collected GPS Information is batched on the device, encrypted, and transmitted to Apple over a secure Wi-Fi Internet connection (if available) every twelve hours with a random identification number that is generated by the device every twenty-four hours. The GPS Information cannot be associated with a particular customer or device.

The collected GPS Information is stored in a database accessible only by Apple.

C. iAd Network

On July 1, 2010, Apple launched the iAd mobile advertising network for iPhone and iPod touch devices running iOS 4. The iAd network offers a dynamic way to incorporate and access advertising within applications. Customers can receive advertising that relates to their interests ("interest-based advertising") and/or their location ("location-based advertising"). For example, a customer who purchased an action movie on iTunes may receive advertising regarding a new action movie being released in the theaters or on DVD. A customer searching for nearby restaurants may receive advertising for stores in the area.

As specified in the updated Policy and the iPhone 4 and iPod touch SLAs, customers may opt out of interest-based advertising by visiting the following site from their mobile device: *https://oo.apple.com*. Customers also may opt out of location-based advertising by toggling the device's location-based service capabilities to "Off."[10]

For customers who do not toggle location-based service capabilities to "Off," Apple collects information about the device's location (latitude/longitude coordinates) when an ad request is made. This information is transmitted securely to the Apple iAd server via a cellular network connection or Wi-Fi Internet connection. The latitude/longitude coordinates are converted immediately by the server to a five-digit zip code. Apple does not record or store the latitude/longitude coordinates—Apple stores only the zip code. Apple then uses the zip code to select a relevant ad for the customer.

Apple does not share any interest-based or location-based information about individual customers, including the zip code calculated by the iAd server, with advertisers. Apple retains a record of each ad sent to a particular device in a separate iAd database, accessible only by Apple, to ensure that customers do not receive overly repetitive and/or duplicative ads and for administrative purposes.

In some cases, an advertiser may want to provide more specific information based on a device's actual location. For example, a retailer may want its ad to include the approximate distance to nearby stores. A dialogue box will appear stating: "iAd would like to use your current location." The customer is presented with two options: "Don't Allow" or "OK." If a customer clicks "Don't Allow," no additional location information is transmitted. If the customer clicks "OK," Apple uses the latitude/longitude coordinates to provide the ad application with more specific location information—the information is not provided to the advertiser.

3. Third-Party Applications

In July 2008, Apple launched the App Store where customers may shop for and acquire applications offered by third-party developers for the iPhone, iPad, and iPod touch. Currently the App Store includes more than 200,000 third-party applications covering a wide variety of areas including news, games, music, travel, health, fitness, education, business, sports, navigation, and social networking. Each application includes a description prepared by the developer regarding, among other things, what the application does, when it was posted, and, if applicable, what information the application may collect from the customer.

Any customer with an iTunes account may purchase and download applications from the App Store. Developers do not receive any personal information about customers from Apple when applications are purchased. Only Apple has access to that information.

---

[9] GPS Information is also collected during the short period of time (approximately thirty seconds) when a GPS-enabled device with location-based service capabilities toggled to "On" is searching for a cellular network. This information is sent anonymously to Apple to assist the device with locating an available channel. Apple does not retain this GPS Information in its database.

[10] A customer who opts out of interest-based and location-based advertising may still receive ads. The ads, however, will likely be less relevant to the customer because they will not be based on either interests or location. The customer also may receive interest-based or location-based ads from networks other than the iAd network.

A. Third-Party Developers

Third-party application developers must register as an "Apple Developer" by paying a fee and signing the iPhone Developer Agreement (the "IDA") and the Program License Agreement (the "PLA"). Registered Apple Developers gain access to the software development kit ("SDK") and other technical resources necessary to develop applications for mobile devices.

The current PLA contains several provisions governing the collection and use of location-based information, including the following:

- Developers may collect, use, or disclose to a third party location-based information only with the customer's prior consent and to provide a service or function that is directly relevant to the use of the application (PLA § 3.3.9);
- Developers must provide information to their customers regarding the use and disclosure of location-based information (*e.g.,* a description on the App Store or adding a link to the applicable privacy policy) (PLA § 3.3.10);
- Developers must take appropriate steps to protect customers' location-based information from unauthorized use or access (*id.*);
- Developers must comply with applicable privacy and data collection laws and regulations regarding the use or transmission of location-based information (PLA § 3.3.11);
- Applications must notify and obtain consent from each customer before location data is collected, transmitted, or otherwise used by developers (PLA § 3.3.12); and
- Applications must not disable, override, or otherwise interfere with Apple-implemented alerts, including those intended to notify the customer that location-based information is being collected, transmitted, maintained, processed, or used, or intended to obtain consent for such use (PLA § 3.3.14).

Developers that do not agree to these provisions may not offer applications on the App Store. Apple has the right to terminate the PLA if a developer fails to comply with any of these provisions. (PLA § 12.2.)

Apple reviews all applications before adding them to the App Store to ensure, for example, that they run properly and do not contain malicious code. Apple, however, does not monitor applications after they are listed in the App Store, unless issues or problems arise.

In closing, let me state again that Apple is strongly committed to giving our customers clear notice and control over their information, and we believe our products do this in a simple and elegant way. We share the Committee's concerns about the collection and misuse of all customer data, particularly privacy data, and appreciate this opportunity to explain our policies and procedures.

I will be happy to answer any questions you may have.

The CHAIRMAN. Can I just pop one right in? Excuse me, please, everybody else.

When you say they go up to a certain place and click and they're out, where is that place on their computer? Is it at the top, at the side, bottom? Is it big? Is it little?

Dr. TRIBBLE. We have a settings menu or a settings page that—where you set everything about your phone, from how bright it is to—including the location settings. If you tap on "Location Settings" on that page, it immediately takes you to a page with a switch that says, "Location Services On/Off." It's a slide switch.

The CHAIRMAN. And again, where do they have to go to tap so that they can get that choice? I'm just asking, is it——

Dr. TRIBBLE. Yes.

The CHAIRMAN.—is it something that——

Dr. TRIBBLE. On your home screen, there's an app called "Settings." It has an icon that has some little gears in it. It's the settings for your phone.

The CHAIRMAN. Then it's at the bottom-right?

Dr. TRIBBLE. As we ship the phone, it's on your home screen. On the home screen, there are various apps like mapping and compass

and things like that, or mail. One of those apps is called "Settings." Clicking on that app brings you to the place where the slide switch for "Location Services" can be turned on or off.

The CHAIRMAN. I understand that, sir, and I appreciate it. And I'd appreciate it, actually, if it's possible, if you could send me a picture.

Dr. TRIBBLE. I'd be happy to show you, if you want.

The CHAIRMAN. Just a simple picture.

Dr. TRIBBLE. Yes. Sure.

The CHAIRMAN. You can send it and I'll pay the mail.

[Laughter.]

Dr. TRIBBLE. Happy to do that.

The CHAIRMAN. OK. Thank you very, very much.

On my list, Mr. Bret Taylor, Chief Technology Officer, Facebook.

STATEMENT OF BRET TAYLOR,
CHIEF TECHNOLOGY OFFICER, FACEBOOK

Mr. TAYLOR. Thank you very much.

Good afternoon, Chairman Rockefeller and other members of the Committee.

The CHAIRMAN. Well, they're all here to hear it.

Mr. TAYLOR. I am Bret Taylor. I'm the Chief Technology Officer of Facebook. Thank you for the opportunity to testify today before the Committee.

Facebook is a service that gives people the power to connect and share with one another, reestablishing and strengthening relationships that enrich our lives and our social discourse.

Last week, we were proud to announce that more than 500 million people around the world are now actively using Facebook. While marking this milestone, we also remind ourselves that the people who use Facebook, and their satisfaction, lie at the heart of what we do.

My written testimony highlights three points: First, Facebook and other social technologies are making the Internet a forum for social interaction, sharing information, and building communities. In just a few years, the Internet has been transformed from a useful, but passive, repository of information into a uniquely powerful means of connecting with others and creating communities that better the lives of others.

Since its creation in a college dorm room in 2004, Facebook has contributed to this transformation, growing from a network of a handful of universities to a worldwide community spanning over 180 countries. Facebook has become an invaluable communication tool, enabling individuals to connect for myriad purpose: for connecting with friends and relatives, for charitable causes, in the political realm, for grassroots organization, and for local community-building.

When we reached 500 million users, we asked people who use Facebook to share some of their experiences with the service. Some of these stories are intimate and personal.

Holly Rose, for example, a mother in Phoenix, credits a friend's status message, asking women to check for breast cancer, with her being diagnosed in time to treat the disease. She used Facebook for

support during the treatment, and became an online prevention advocate, herself.

Other stories have broader significance. The 2008 Presidential race has been called "the Facebook election," as candidates relied on the service for developing grassroots support. It's estimated that over 300 Members over Congress use Facebook to communicate officially with constituents, and 22 out of 24 major Federal agencies use Facebook.

By providing tools and services that people can use to build their Internet experience around their personal interests, we're helping to make the Internet more personal and more relevant.

My second point is that one of the primary reasons for Facebook's success is that Facebook provides uniquely powerful controls for sharing information. It is our belief that when people have control over what they share, when they share it, and with whom they share it, they will feel more comfortable sharing. That's why we're not only focused on creating new ways for people to share and connect, but also focused on building innovative new controls for sharing.

The people who use Facebook continuously give us real-time feedback on these product decisions by the choices they make: to join the site, to use our tools, or even to engage less. In this way, it is the people who use Facebook that ultimately drive all of our product decisions.

Recent changes we've made offer great examples of these innovative new controls. In my written testimony, I highlight four recent changes: the privacy transition tool, the contextual privacy control, the one-click-sharing control, and granular-data permissions. I'm happy to discuss any and all of these in response to your questions.

And finally, I want to highlight the important economic growths created and supported by the people who use Facebook and those companies that innovate by building on Facebook's social platform. The growing economic vitality of the Internet makes Facebook—the Facebook experience possible and free of charge to our users without Facebook ever sharing personally identifiable information with advertisers.

Facebook is a U.S.-based company. Even though 70 percent of Facebook users are outside the United States, more than 80 percent of its employees are located here.

But, this is only a fraction of Facebook's economic impact. In 2007, we launched the Facebook platform, which enables developers to deploy innovative and social applications to Facebook's large user base. The explosion of innovation and activity has created an entire economy around the platform. More than a million applications are now available on the platform. Some of these applications are built with businesses that employ hundreds of people and make hundreds of millions of dollars in revenue.

As just one example, the New York Times ran an article this weekend about a leading Facebook games developer called Zynga. Zynga has nearly 1,000 employees, up from 375 a year ago, and now has 400 job openings. The company has been valued at over $4.5 billion.

Another Facebook developer, Playfish, was acquired by Electronic Arts for an estimated $400 million in 2009.

These are two of the largest success stories in Facebook's platform economy, but we see many others coming, as well.

In conclusion, I want to emphasize that the real power of Facebook lies with the individuals who use the service to connect and share with their friends and engage with the world around them. We're proud of the service we provide them. And using innovative technologies, Facebook will continue to facilitate a more personalized, more engaging Internet experience.

I am grateful for the opportunity to be here, and I look forward to your questions.

[The prepared statement of Mr. Taylor follows:]

PREPARED STATEMENT OF BRET TAYLOR, CHIEF TECHNOLOGY OFFICER, FACEBOOK

Good afternoon, Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee. I am Bret Taylor, Chief Technology Officer for Facebook. Thank you for the opportunity to be here today to testify before the Committee.

Executive Summary

Facebook is a service that enables people to connect and share with one another, forming and deepening relationships and communities that enrich their lives and our social discourse as a whole. Last week we were proud to announce that more than 500 million people all over the world are now actively using Facebook. We take pride in this growth because we are empowering people to share and connect with the world around them. While marking this milestone, we also remind ourselves that the people who use Facebook and their satisfaction lie at the heart of what we do.

In my testimony today I will address three topics. *First*, I will describe how Facebook and other social technologies are making the Internet a forum for social interaction, sharing information, and building communities. In just a few years the Internet has been transformed from an isolated, passive, and anonymous experience into a uniquely powerful means of connecting with other people, deepening personal relations, and creating communities that better the lives of others.

Second, I will discuss how user control and responsiveness are essential to sharing and connecting using Facebook. The people who use Facebook supply Facebook's content, and are the driving force behind the continued innovation and constant improvement of our service. Our goal is to make it simpler for people to connect and share, and to give them the tools to control their information.

Third, I will describe the important economic growth created and supported by the people who use Facebook and by those companies that innovate based on Facebook's social technology. Facebook provides a platform for thousands of entrepreneurs to develop, offer, and market valued products and services to people across the globe. We connect advertisers with people in a way that is unobtrusive, and that enables the advertiser to direct information toward the people who are most likely to find it relevant and valuable. We do this without selling user information to advertisers or giving advertisers access to personal information.

1. The Transformative Effect of Social Technology

The Internet now connects nearly 2 billion people around the world.[1] Until recently, though, the Internet was an isolated, one-way, one-dimensional experience. Users visited websites, read articles, and gathered information, but had little if any meaningful interaction with one another on the web. Internet communications that did occur often were anonymous, with users' identities obscured by pseudonyms or meaningless sequences of letters and numbers. The Internet was responsive to users' requests and instructions, but it was not truly interactive.

In a few short years the Internet has evolved from an impersonal, anonymous medium to an interactive social experience defined by a person's connections, interests, and communities. That transformation has occurred in tandem with what has been called "Web 2.0," an explosion in innovative functionalities that could not have been imagined during the Internet's infancy. These developments provide interactive experiences and allow users to generate and define relevant content. They enlist people as both the viewers and creators of online content, frequently in a framework

[1] *Internet Usage Statistics, The Internet Big Picture*, World Internet Users and Population Stats, *http://www.internetworldstats.com/stats.htm*.

that is social and involves open forums or communities defined by the users themselves.

Since its creation in a Harvard dorm room by Mark Zuckerberg in 2004, Facebook has been at the forefront of this change, growing from a network at a handful of universities to a worldwide community of users in over 180 countries. As Facebook has expanded, we have also continually innovated and implemented new tools for users, responding to the immense public demand for more and better ways to share and connect. These immensely popular innovations include a photo-sharing feature that, with some 50 billion pictures online, constitutes the largest photo archive in the world; a "Wall" feature through which users can post messages on their friends' individual pages; and the "News Feed," which provides users up-to-the-minute interactive content based on updates by the user's friends and his or her interests and communities. Each of the 500 million people that use Facebook experience their own personalized homepage and News Feed when they go to *Facebook.com,* connecting them to their own community of friends and interests.

Facebook and other social technologies have the power to enrich users' lives—and society as a whole—in ways that were un-imagined 5 years ago. Families and friends in locations across the globe are in closer contact than ever before and can more easily follow issues, people, and causes of interest to them; identify others who share their enthusiasms; and deepen their knowledge and understanding of their world. Facebook has become an invaluable communication tool, allowing individuals to connect for myriad purposes—for charitable causes, in the political realm, for grassroots organization, and for local community building.

To celebrate the 500 million people that have been empowered and connected by Facebook, last week we launched a new application called Facebook Stories (*stories.facebook.com*), which allows individuals to share stories about how Facebook has enriched their lives. Among the thousands of examples we have received are the following:

- Ben Saylor, a 17-year-old high school student, turned to Facebook to organize a community effort to rebuild the oldest outdoor theater in Kentucky, which had been damaged by floods in May.
- Holly Rose, a mother in Phoenix, credits a friend's status message asking women to check for breast cancer with her being diagnosed in time to treat the disease. She used Facebook for support during the treatment and became an online prevention advocate herself.
- Many have now even begun using Facebook to reach out to their communities to find organ donors—Sarah Taylor of Pennsylvania quickly found a kidney donor after spending 8 years in renal failure.

As more and more people join and use Facebook, the possibilities for individual and collective action will multiply almost exponentially.

Facebook and other social technologies have even played a key democratic function at home and abroad. Because these services allow users to quickly share information and build communities, democratic organizers have embraced Facebook as a key tool in places such as Iran and Colombia.[2] Government leaders and policymakers are now using Facebook to communicate with citizens.

- In the U.K., Prime Minister David Cameron launched a "crowdsourcing" initiative to seek out citizen proposals on cutting government spending. On a web conference with Mark Zuckerberg, Prime Minister Cameron thanked Facebook for providing the medium for such an initiative.[3]
- Here at home, the 2008 Presidential race has been called the "Facebook Election," as President Obama and Senator McCain relied on the service for developing grassroots support, and Facebook cosponsored one of the Presidential debates (together with a traditional media outlet, ABC News).[4]

---

[2] Lev Grossman, *Iran Protests: Twitter, the Medium of the Movement*, Newsweek, June 17, 2009; Sibylla Brodzinsky, *Facebook Used to Target Colombia's FARC with Global Rally*, CHRISTIAN SCI. MONITOR, Feb. 4, 2008.

[3] Gina Lovett, *Government Drafts in Facebook for Second Crowdsourcing Initiative*, NEW MEDIA AGE, July 9, 2010, *http://www.nma.co.uk/news/government-drafts-in-facebook-for-second-crowdsourcing-initiative/3015666.article*.

[4] Brian Stelter, *ABC News and Facebook in Joint Effort to Bring Viewers Closer to Political Coverage*, N.Y. TIMES, Nov. 26, 2007; Virginia Heffernan, *Clicking and Choosing: The Election According to YouTube*, N.Y. TIMES, Nov. 14, 2008; Matthew Fraser & Soumitra Dutta, *Barack Obama and the Facebook Election*, U.S. NEWS AND WORLD REP., Nov. 19, 2008.

- It is estimated that more than 300 Members of Congress use Facebook in their official capacity.[5]
- Even Federal agencies have adopted Facebook as a powerful communication tool—22 out of 24 major Federal agencies use Facebook.[6]

In these and other ways, Facebook has become an integral part of everyday communication and community-building across the globe. Continual innovation and new technologies have been essential to this. These innovations and new technologies are designed to improve not only how people interact with one another on the Internet, but also how they interact with the Internet itself. By providing tools and services that people can use to build their Internet experience around their personal interests, we help make the Internet more responsive and relevant to them even when they visit sites other than Facebook.

To that end, in 2007 Facebook launched Facebook Platform, which allows developers to create innovative social applications and make them available to people who use Facebook. This innovation made Facebook an entry point to a new universe of tools, experiences—and of course, games—that deepen the connection among people on the Internet. The hundreds of thousands of applications made available through Facebook Platform include the following:

- The *Causes* application, which provides an online platform for individuals and organizations to raise funds for charitable causes.
- The *Circle of Moms* application, a local support group for mothers that draws on the collective knowledge of the community for support.
- The *Birthday Calendar* application, which allows you to track birthdays, anniversaries, and other important dates of friends.

These developments on Facebook Platform go beyond mere socializing, and provide real, meaningful interactions for people who use Facebook.

Earlier this year we extended Facebook Platform to offer this connectivity and customization to other sites on the Internet. In April, we introduced "social plugins," easy-touse tools that allow previously generic websites to become customized to an individual's interests and network of friends and associations. For example, a Facebook user visiting a website can instantly share content of interest by clicking on the Facebook "Like" button, which can bring that content to the attention of the person's friends on their real-time News Feed on their home page, and when they visit the same site. With social plugins, websites are instantly made more social, interactive, and relevant to the individual; as people move through the Internet, websites increasingly reflect their body of relationships and connections on the Internet.

This customization can be seen on many of the Internet's most frequently visited websites. The popular movie database, IMDb, which previously served simply as a repository of movie information, now offers a way for friends to share information about their favorite movies and actors. Traditional news outlets, such as CNN and the *Washington Post*, have also adopted the power of the social network, offering the ability to access tailored and personalized news sources. Instead of wading through an entire newspaper, people who use Facebook now have the option to focus on the information that is relevant in the context of their interests and connections, in much the same way that Members of this Committee are greeted in the morning by news clips that have been selected according to issues of special importance to you and your constituents. Facebook's "Like-button has become a ubiquitous feature of the web, allowing individuals to quickly and easily share their favorite parts of the Internet with their friends and broader communities.

As Mark Zuckerberg put it at the conference where Facebook launched these social plugins, "Our goal is [for] people [to] have instantly social experiences wherever they go."[7] At the same time, social plugins do not require any personal information to pass from Facebook to an external website. Plugins promote a tailored Internet experience, while maintaining user control over personal information. Since the launch of social plugins in April of this year, they have been incorporated by more than 350,000 websites, bringing a more personalized Internet to millions.

---

[5] Posting of Tony Romm to The Hill, *"Congress on Facebook' Goes Live, http://thehill.com/blogs/hillicon-valley/technology/97683-congress-on-facebook-goes-live* (May 13, 2010 7:58 EDT).

[6] *Information Management: Challenges in Federal Agencies' Use of Web 2.0 Technologies, Hearing Before the Subcomm. on Information Policy, Census, and National Archives of the H. Comm. on Oversight and Government Reform*, 111th Cong. (July 21, 2010) (statement of Gregory C. Wilshusen, Director of Information Security Issues, Government Accountability Office).

[7] Mark Zuckerberg, CEO, Facebook, Inc., Remarks at f8 Developers' Conference, Apr. 21, 2010.

Facebook is now offering a pilot program, Instant Personalization, which will allow individuals to have a more robust personalized experience with partner sites, initially Yelp, Pandora, and Microsoft Docs.com. These sites now provide a truly personal and tailored experience to visitors as soon as they arrive. These innovations address people's real frustration with the static, anonymous Internet of the past. Instead of visiting a generic website and wading through a lot of irrelevant content, Instant Personalization makes it possible for you to go to a site and immediately receive content that is relevant to you and your friends, the place you live, and the things you like to do. By offering personalized service, these partner sites experience greater engagement from people who use Facebook.

For example, the website Yelp already offered a valuable service by compiling user reviews of restaurants, bars, clubs, and other services. These reviews could come from any reviewer, anywhere on the Internet. Through Facebook's Instant Personalization, Yelp became a tailored experience that is even more relevant and useful. While you can still read generic reviews on the site, you can also now choose to focus on reviews by your friends and acquaintances. By enabling you to learn the favorite restaurants of people you trust in a city you're visiting for the first time, Instant Personalization immeasurably increases the value of the site.

Similarly, the music streaming service Pandora already offered a highly personalized service by using advanced algorithms to tailor music playlists to your tastes—based on the music you currently listen to, Pandora introduces you to new music that you're also likely to enjoy. By adopting Instant Personalization, Pandora can magnify the personalization of this experience by identifying music through the lens of your social networks. People have long relied on friends, coworkers, and relatives for music recommendations; now Pandora can enhance this experience online with the help of Facebook. Of course, Facebook has worked diligently to provide multiple and meaningful opportunities for users to learn about and choose to participate in Instant Personalization, and to ensure that our partners adopt and enforce adequate protections for personal information.

2. Facebook's Focus on User Control and Responsiveness

People are at the heart of what we do at Facebook. On Facebook, individuals provide the content—they have the freedom to share what they want, when they want, and how they want. As a result, Facebook is personalized to each individual user. Unlike other web companies, Facebook does not offer a single homepage; each of the 500 million people that use Facebook has their own personalized News Feed, customized to their interests, friends, and communities. For these reasons, user control has always been integral to Facebook. People who use Facebook determine what content is shared and how it is shared. Facebook is built from the bottom up, taking what we call a hyper-grassroots approach to sharing information.

People who use Facebook are engaged in building a safe, secure experience for themselves and their friends. As a result, we have developed powerful mechanisms for self-regulation and user protection. Individuals use social technologies to connect and share information, but they also play an important role in policing the medium itself. In fact, users are actively involved in monitoring and controlling their online presences, and can often provide the best check on a company's information sharing policies. An important recent study by the Pew Research Center found that 57 percent of adult Internet users monitor their online presence.[8] Among users age 18 to 29, 71 percent have adjusted their settings and controls to regulate how much they are sharing with others, and 65 percent of all social-networking site users have done so.[9] If these users feel that a service is overstepping its bounds, they will actively take steps to control their own personal information.

Facebook continually seeks to improve our user interface, our data-sharing policies, and the overall experience of people who use our service. Recent changes to Facebook's controls and privacy policy provide a prime example of how social technologies have a dynamic ability to respond to users and self-correct. Over the last year, Facebook has continued to innovate new ways to offer simpler and better controls:

- *Privacy Transition Tool.* When Facebook introduced a new privacy framework in December of last year, we took the unprecedented step of requiring all users to navigate through a privacy "transition tool" to confirm their settings for sharing information and to change the settings if they chose. Instantly, hundreds of millions of individuals took time to meaningfully engage with the concept of

[8] MARY MADDEN & AARON SMITH, PEW INTERNET & AMERICAN LIFE PROJECT, PEW RESEARCH CENTER, REPUTATION MANAGEMENT AND SOCIAL MEDIA 8, 21 (May 26, 2010).

[9] *Id.*

privacy and consider whether their settings accurately reflected their preferences, in a manner that had never occurred before, on or off the Internet.

- *Contextual Privacy Control.* Also last year, Facebook deployed a contextual privacy control, which allows people to control who will see their content when it is shared. Like the transition tool, Facebook sought to maximize both simplicity and control, a delicate balance, while assisting each user to select the extent of sharing that makes them feel comfortable.
- *One-Click Sharing Control.* In April, Facebook offered a new simplified control for sharing that lets people control over twenty categories of information with just one click. Facebook implemented these changes and additions to its controls working quickly—in the face of enormous technical complexity—to respond to views expressed in the user community. In addition, Facebook offered an easy way for people to control the access that Platform developers have to their information.
- *Granular Data Permissions.* In June, Facebook became the first provider to require developers to obtain "granular data permissions." Developers using Platform must now specifically request data directly from the individual—who retains the ultimate simple choice of whether to share information with an outside developer. This granular permissions model actually gives people more control over their information than comparable services, while allowing developers to continue the vibrant innovation that has marked the Platform economy.

To facilitate responsiveness to users, Facebook introduced a "notice and comment" process for vetting some of its potential changes, modeled in part on the Federal Government's rulemaking procedures. This process also serves to educate and engage users about potential policy changes. At times we will even hold a user vote on proposed policy changes, as we did in April when we issued our Statement of Rights and Responsibilities and revised Privacy Policy. We are aware of no Internet-based company, large or small, that goes to such lengths to publicize and incorporate individuals' feedback into those key documents. It is a further reflection of our commitment to hearing peoples' voices in the governance of their community. This commitment translates into real practical tools that people can and do use.

As we move forward, the people who use Facebook will continue to shape our future by how they balance their demand for sharing and connection on the one hand, with their desire to control the content they share on the other hand. just as we innovate new ways for sharing and connection, we also innovate new ways to offer users control. And, of course, the people who use Facebook also retain control over the service and offer us real-time feedback by the choices they make—to join, to leave, to use our tools, or to engage less. In this way too, it is the people who use Facebook that ultimately drive our innovation.

Such innovation is essential to the Internet, yet the best innovations can be unexpected—they can surprise. This was the case with Facebook's News Feed, which gives users a real-time and interactive "ticker" of the updates and content their friends are sharing on Facebook, along with customized content related to the interests the user has identified and the associations he or she has formed on the Internet. The News Feed is integral to the connectivity, personalization, and immediacy of the Facebook experience and today is among our most popular features, but when it was introduced in 2006 it initially drew strong opposition from a large number of Facebook users. Appropriately, some formed Facebook groups against the News Feed. We listened, made some modest changes, and now most Facebook users could not imagine our service without it.

Facebook is thus an example of the tremendous self-corrective capacity of Internet-based services, particularly with respect to the balance between openness and privacy. Facebook's response to user feedback has helped it to become a better service while continuing to enhance the user experience and pioneer new ways to share information. And, Facebook's pioneering development of user controls for the information they share is an example for regulators in the U.S. and abroad of how approaches that vest decisionmaking in individual users, rather than in government regulators, are the most promising means of furthering user satisfaction and Internet innovation.

Of course, the involvement of the Federal Government is also needed, for example, to guard against criminals and miscreants who would leverage the Internet's openness to engage in scams, identity theft, and other activities that cause financial or even physical harm. That is why we applaud Congress for enacting targeted statutes that address those problems without cabining the creative freedom that is the

life force of the Internet. The Computer Fraud and Abuse Act,[10] the Child Online Privacy Protection Act,[11] and the Controlling the Assault of Non-Solicited Pornography and Marketing Act (the "CAN–SPAM" Act)[12] all have served to protect the public from some of the Internet's dangers and annoyances.

Facebook often works arm-in-arm with the government in these areas. For example, it has invoked the CAN–SPAM Act vigorously to defend its users against malicious online attacks and to help make the Internet safer for all by taking spammers out of commission: we have obtained the two largest-ever civil judgments under the Act.[13] We are also proud that last year TRUSTe, a nonprofit privacy standard-setting organization, rated Facebook one of its ten most trusted companies based on a public survey and an expert review.[14]

Facebook and other social technologies are increasingly important forums for public communication, speech, and debate on a broad range of social and even political matters. Our country's traditions appropriately include a great hesitancy to regulate communication and the sharing of information in such areas. We believe that Congress's approach toward the Internet to date, which has avoided open-ended grants of regulatory authority or over-inclusive prohibitions, should serve as a model for any future legislative initiatives. As always is the case, it will be valuable for Congress to build an evidentiary record establishing the need for intervention before it acts. Overbroad or burdensome regulation carries the risk of stifling the innovation that is the lifeblood of the Internet and has served as a major source of jobs and economic growth.

To conclude on this topic, user control is central to how Facebook operates, and will remain so. We share the commitment of Congress to ensure a safe, secure Internet experience, while facilitating the innovation and sharing of information that people expect. We value our relationships with the Federal Government, with states, and with enforcement agencies throughout the world, and will continue to work with Congress and others to ensure that our users, especially young people, have a safe and productive Internet experience.[15]

3. Facebook's Economic Role for Users and American Business and Workers

Facebook and its leadership are driven by a vision of the Internet's capacity to make the world more connected, enriching our personal lives, our society, even our democracy. But of course the Internet is also an important economic presence, particularly in these challenging economic times. It is this economic vitality that makes the Facebook experience possible and free of charge to our users, without Facebook ever sharing personally identifiable information with advertisers.

In 2009, online retail spending in the United States was nearly $130 billion, only slightly lower than in 2008 despite the enormous impact of the recession on the U.S. economy.[16] One estimate suggests that the commercial Internet adds $1.5 trillion in value to businesses and consumers worldwide.[17] And in a time of economic hardship, Web 2.0—and social networking services in particular—are providing a much needed source of jobs, growth, investment, and innovation. Facebook is a U.S.-based company—even though 70 percent of Facebook users are outside of the United States, 80 percent of its employees are located here. The Chairman of the Federal Communications Commission recently recognized how the entrepreneurial power of services like Facebook can drive economic growth and create jobs here at home.[18]

---

[10] Pub. L. No. 99–474, 100 Stat. 1213 (Oct. 16, 1986).

[11] Pub. L. No. 105–277, 112 Stat. 2581 (Oct. 21, 1998).

[12] Pub. L. No. 108–187, 117 Stat. 2699 (Dec. 16, 2003).

[13] A 2008 judgment against Adam Guerbez and Atlantis Blue Capital ($873 million) and a 2009 judgment against the "Spam King" Sanford Wallace ($740 million).

[14] TRUSTe, *Press Release: 2009 Most Trusted Companies in Privacy*, Sept. 16, 2009.

[15] Facebook offers its service to people age 13 and over. We clearly describe this age limit in our Privacy Policy, and if we learn that a child under 13 has shared information on our service, we will delete that information as quickly as possible. *See also The Role of Innovation in Creating a Safer Online Environment—The Facebook Experience, Before the Subcomm. on Consumer Protection, Product Safety, and Insurance of the S. Comm. on Commerce, Science, and Transportation*, 111th Cong. (2010) (Testimony of Timothy Sparapani, Director, Public Policy, Facebook), available at *http://commerce.senate.gov/public/?a=Files.Serve&File_id=dac6055f–274c–4813–955a414ccd0c4b3a*.

[16] Jeff Clabaugh, *Online Spending in 2009 Falls*, MILWAUKEE BUS. J., Feb. 9, 2010.

[17] ROBERT D. ATKINSON ET AL., THE INFO. TECH. & INNOVATION FOUND., THE INTERNET ECONOMY 25 YEARS AFTER .COM 1, 4 (2010).

[18] Referring to Facebook, FCC Chairman Julius Genachowski noted the power of the Internet's "distributed innovation and ubiquitous entrepreneurship," which creates "jobs and opportunity everywhere there is broadband." Julius Genachowski, Chairman, Fed. Comms. Comm'n, Pre-

Continued

Facebook Platform, which helps create innovative and more personalized experiences for users, also serves American businesses and workers by fostering what is in a sense an entire Platform economy. It is a marketplace to which hundreds of thousands of third-party developers may bring their ideas and inventions and offer them to Facebook users. More than half a million applications are now available on Platform. Some of these applications are associated with businesses that employ hundreds of people and have hundreds of millions, even billions of dollars in value:

- Leading games developer Zynga, creator of the popular Farmville game that was developed on Facebook Platform, has nearly 1,000 employees, up from 375 employees a year ago, and now has some 400 job openings. Its games have 211 million players every month (according to AppData.com's count), and the company has been valued at more than $4.5 billion.[19]
- In 2009, games developer Playfish was acquired by Electronic Arts for an amount reported to be as much as $400 million. Although based in the U.K., Playfish has developed a substantial presence in the United States, which includes at least four development studios.[20]

This vibrant economy of features and applications has shattered the barriers that may have previously limited what one company could offer to users. Facebook for its part helps protect users' Platform experience by arming users with control over the information applications receive, through rigorous policies and technical controls that apply to our Platform, and in reviews and investigations conducted by our Platform Operations Team.

Online advertising is of course a critical component of the economic growth that the Internet has spurred. As mentioned, it also enables Facebook to offer its service for free, without ever sharing personally identifiable information with advertisers. Facebook believes that social advertisements complement the way people already use Facebook to discover, share, and connect with people and the world around them. Whether it's a new car, clothes, or music, many of the things people discover on the Internet come from their friends—through Facebook, advertisers can complement what people learn from their friends in an unobtrusive way.

We achieve this by only providing advertisers with anonymous, aggregated data. We ask advertisers to identify characteristics of users they wish to advertise to, such as age, gender, or location. Facebook then itself distributes those advertisements to the appropriate audience on its site, without ever disclosing personally identifiable information to its advertisers. After the advertisements run, Facebook will provide a report to the advertiser so they can measure the success of their ads—these reports, too, contain no personally identifiable information.

This model allows consumers and businesses alike to enjoy the efficiencies of personalized advertising, while protecting personal information. The advertisements that result—which are a far cry from the annoying pop-ups and flashing banner ads of days past—provide people with relevant and targeted commercial messages that further growth and innovation on the Internet.

Conclusion

The 500 million people across the globe that actively use Facebook have made the world a more open and connected place. They have driven innovation in ways that few would have predicted a decade ago; the promise of this thriving community is limitless. But the real power of Facebook lies with the individuals who use the service to connect and share on a daily basis. Facebook seeks to remake the Internet for them and for those who have yet to join. We will continue to show leadership in giving people greater control over personal information. And using innovative technologies like social plugins and the economic catalyst of social advertising, Facebook will continue to facilitate a more personalized, more responsive Internet experience.

The CHAIRMAN. Thank you very much, Mr. Taylor.

And next on my list here is Dr. Whitten, Privacy Engineering Lead, Google.

---

pared Remarks at the Brookings Institute (Sept. 21, 2009), available at *http://www.openInternet.gov/readspeech.html* (emphasis added).

[19] Miguel Helft, *Will Zynga Become the Google of Games?*, N.Y. TIMES, July 24, 2010.

[20] Erick Schonfeld, *Not Playing Around. EA Buys Playfish for $300 Million, Plus a $100 Million Earnout*, TECHCRUNCH, Nov. 9, 2009.

STATEMENT OF DR. ALMA WHITTEN,
PRIVACY ENGINEERING LEAD, GOOGLE INC.

Dr. WHITTEN. Thank you, Chairman Rockefeller, Senator Kerry.

I've devoted my career, both as an academic and now as Google's lead privacy engineer, to one primary goal: making it intuitive, simple, and useful for Internet users to take control of their privacy and security. This is the central challenge of privacy engineering.

Products and services, particularly on the Internet, constantly evolve. Valuable new services, from social networking to online video to mobile computing, change the way that we interact with each other and use information. These services, built in part from the information that providers learn from their users, offer tremendous value. Many are offered for free.

They certainly have been good for our economy. In 2009 alone, Google's search and online advertising generated a total of $54 billion of economic activity for American businesses, Website publishers, and nonprofits, including over $5 billion of revenue that we paid to publishers last year. And that's not to mention the positive economic impact of our free products, like Gmail and YouTube.

Google's greatest asset is our users' trust. The information that our users entrust to us enables us to better match searchers to the information that they seek; to fight off those who would scam our users or undermine the usefulness of our search results, and to create new services, like translation, speech to text, and many others. We focus on building transparency, user control, and security into our products. And we constantly renew, innovate, and iterate to make sure that we are honoring our users' privacy expectations and security needs. And, because our users' trust is so critical to us, it's important for us to note that we do not sell our users' personal information.

The Google Dashboard is a cornerstone of our efforts. If you haven't seen this tool, I urge you to take a look at google.com/dashboard. We developed the Dashboard to provide users with a one-stop, easy-to-use control panel for the personal information associated with their Google accounts, from Gmail to Picasa to Search to more than 20 other Google products. With the Dashboard, a user can see, edit, and delete the data stored with her individual Google account. She can change her privacy settings, see what she is sharing and keeping private, and click into the settings for any individual product.

I was adamant, when we created the Dashboard, that we not make it seem strictly a privacy tool. I wanted it to be, above all, a useful tool that our users would come back to and interact with, even if they were not consciously thinking about privacy.

We took a similar approach with our advertising network. Our Ads Preferences Manager, which is linked from every ad in our advertising network, allows users to opt out of ad targeting and to learn about our privacy practices. But, equally important, it allows users to look at the categories of ads that they will see, select new interest categories, and remove ones that don't match their interests. By offering this useful service, we hope to get more people to understand and confirm their privacy settings. Interestingly, for every one user who opts out, we see four edit their preferences, and ten view the page and do nothing.

These are great examples of transparency and control designed into products in a way that is prompting individual users to learn more about how to control their information. And we're proud of this track record. However, despite our best efforts, on occasion we have made mistakes.

In May, Google disclosed that we had mistakenly included code in the software on our Street View cars that collected samples of Wi-Fi payload data, information sent over a network from open unencrypted Wi-Fi networks. To be clear, Google never used the mistakenly collected data in any product or service, and there was no breach or disclosure of any personal information to any third party. And as soon as we learned about this incident, we disclosed what had happened and acknowledged our mistake.

Google is working hard to fully and completely address this incident. We need to do better. We are taking the review of this matter very seriously, and we will announce the changes that we will make to prevent such a thing from happening in the future.

At the same time, we continue to develop industry-leading privacy and security tools. For instance, we recently launched encrypted search, allowing users worldwide to protect their search queries from snooping or interception. We are also the only major Webmail provider to encrypt all e-mail traffic, by default. This is the proactive approach that my team brings to our jobs, and the goal of all of us at Google.

I look forward to answering your questions. Thank you.

[The prepared statement of Dr. Whitten follows:]

PREPARED STATEMENT OF DR. ALMA WHITTEN, PRIVACY ENGINEERING LEAD, GOOGLE INC.

Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee:

I am pleased to appear before you this afternoon to discuss online privacy and the ways that Google protects our users' personal information. My name is Dr. Alma Whitten, and I am Google's Privacy Engineering Lead. I am responsible for a team of dedicated privacy and security engineers who develop and improve Google's privacy tools, like our Dashboard, and work with our other engineers and product teams to build transparency, user control, and security into Google's products.

Google is most well known for our search engine, which is available to Internet users throughout the world. We also offer dozens of other popular services, from YouTube to Gmail to Google Earth. Our products are free to individuals for personal use, supported by revenue from online advertising.

While our users benefit from our free services, Google's innovative advertising system is also helping businesses grow in a challenging economic time. In 2009 alone, our advertising products generated a total of $54 billion of economic activity for American businesses, website publishers, and non-profits. This number only covers economic activity generated by Google's search and advertising tools, including the over $5 billion of revenue we generate for online publishers in 2009. It does not include the positive economic impact of products like Gmail and others that allow consumers, entrepreneurs, and businesses of all sizes to communicate and collaborate for free—or, in the case of enterprise customers, at a lower cost than alternative platforms.

Our recent economic impact report (*google.com/economicimpact*) explains Google's contribution to the American economy, and features small businesses that rely on Google's advertising products to reach customers and generate revenue.

One example is OVIS, a 20 year-old cabinet hardware and woodworking supplier based in Millwood, West Virginia (*www.ovisonline.com*). OVIS's owner Chip Wimbauer told us that Google's advertising system is "the best way for a small business to compete and look like a big company," and that with online advertising OVIS has gone from a regional company to one that does as much business in Hawaii as it does within West Virginia. In Texas last year we created over $3 billion

in economic value for over 100,000 advertisers and online publishers. And we donated almost $3 million in advertising to non-profit groups like the American Heart Association and the Susan G. Komen Breast Cancer Foundation through our Google Grants program (information about which is available at *www.google.com/grants*). These types of success stories happen in every state in partnership with hundreds of thousands of businesses and numerous not-for-profit organizations.

In a time of tight budgets, we're glad to help so many small businesses and entrepreneurs find customers more efficiently and increase revenue through relevant advertising. We also take pride in building trust with users, and privacy is a core part of that effort.

At Google, privacy is something we think about every day across every level of our company. We make this effort because privacy is both good for our users and critical for our business. If we fail to offer clear, usable privacy controls and strong security, our users will simply leave. This is the basic truth that guides me in my job as Google's lead privacy engineer.

In my testimony today, I'm going to talk about three topics:

First, I'd like to discuss how Google's approach to privacy manifests itself in our products. In other words, how do we put our privacy principles into executable code? I'll provide several examples to give the Committee a tangible sense of the considerations that go into designing privacy as part of our products and the transparency, control, and security that are built into Google's products.

Second, I will discuss the challenges companies like Google face when designing for privacy and security. How do we harness the power and value of data for our users while protecting against privacy harms? How can we communicate about evolving data practices and controls to users in a meaningful way?

Third, while I'm far from a legal expert, I'll offer a bit of thought as to how Congress can help protect consumers and improve user trust in data-intensive services—including through the development of comprehensive, baseline privacy rules.

How We Approach Privacy at Google

When I think about privacy at Google, I start with our five privacy principles. In brief, these are:

- Use information to provide our users with valuable products and services.
- Develop products that reflect strong privacy standards and practices.
- Make the collection and use of personal information transparent.
- Give users meaningful choices to protect their privacy.
- Be a responsible steward of the information we hold.

The principles are located at *www.google.com/corporate/privacy_principles.html*.

Let's break these down a bit. As with every aspect of our product, we follow the motto of "Focus on the user and all else will follow." We are committing ourselves to use information only where we can provide value to our users. That's what we mean by our first principle.

For instance, *we do not sell our users' personal information*.

To further guide us, under the second principle, we aim to build privacy and security into our products and practices from the ground up. From the design phase through launch we are considering a product's impact on privacy. And we don't stop at launch—we continue to innovate and iterate as we learn more from users.

Our last three principles give substance to what we mean by privacy: We commit to *transparency, user control*, and *security*.

We work hard to embed privacy considerations into our culture through our principles and in the way we're organized. As Google's Privacy Engineering Lead, I'm only one of many individuals at the company who work on privacy from every angle—including technology, products, policy, and compliance initiatives. This cross-functional team, all focused on our users' privacy interests, ensures that privacy doesn't exist as a silo within Google. For example, our Privacy Council, a cross-functional group of Google employees, helps us identify and address potential privacy issues across all our products.

In just the last 18 months, we have been tackling four broad privacy issues that face our industry in a way that is consistent with our principles:

- Transparency and control in the online advertising ecosystem.
- Easy data portability for information that is processed and stored by Google.
- A comprehensive and useful dashboard of privacy and account controls for a suite of web services.

- Strong security for users of Google's services, like Gmail and Google Search.

In the next section of my testimony I'll discuss these privacy issues and illustrate how Google works to bring transparency, user control, and security to its users.

Transparency and Control for Interest-based Advertising

The availability of Google Search and our other products—and the improvements that we make to our products on a daily basis—is funded by online advertising: by far our primary source of revenue. As we work to bring more relevant ads to our users, we continually seek to preserve transparency and user control over the information used in our ad system.

Google was not the first to offer interest-based advertising (known as IBA) online, but it was important to us that we offer clear and strong privacy controls before introducing this product. When we launched IBA, in March 2009, we included a number of groundbreaking privacy features. As Google *tells its users*:

> Many websites, such as news sites and blogs, use Google's AdSense program to show ads on their sites. It's our goal to make these ads as relevant as possible for you. While we often show you ads based on the content of the page you are viewing, we also developed new technology that shows some ads based on interest categories that you might find useful.

Google's interest-based ads contain notice in the actual advertisement indicating that it is a Google ad. The in-ad notice is linked to information about IBA, including our Ads Preferences Manager, which allows users to change the interest categories used to target ads or to opt-out of interest-based advertising altogether. Note that we use only non-personally-identifiable data for IBA targeting.

Fig. 1: Sample advertisement with in-ad privacy notice

With the launch of our Ads Preferences Manager (*www.google.com/ads/preferences*), Google became the first major industry player to empower users to review and edit the interest categories we use to target ads. The Ads Preferences Manager enables a user to see the interest categories Google associates with the cookie stored on her browser, to add interest categories that are relevant to her, and to delete any interest categories that do not apply or that she does not wish to be associated with.

I should also clarify that Google does not serve interest-based ads based on sensitive interest categories such as health status or categories relating to children under 13.

The Ads Preferences Manager also permits users to opt out of interest-based ads altogether. Google implements this opt-out preference by setting an opt-out cookie that has the text "OPTOUT" where a unique cookie ID would otherwise be set. We have also developed tools to make our opt-out cookie permanent, even when users clear other cookies from their browser (see *www.google.com/ads/preferences/plugin*). We are encouraged that others are using the open-source code for this plugin, released by Google, to create their own persistent opt-out tools.

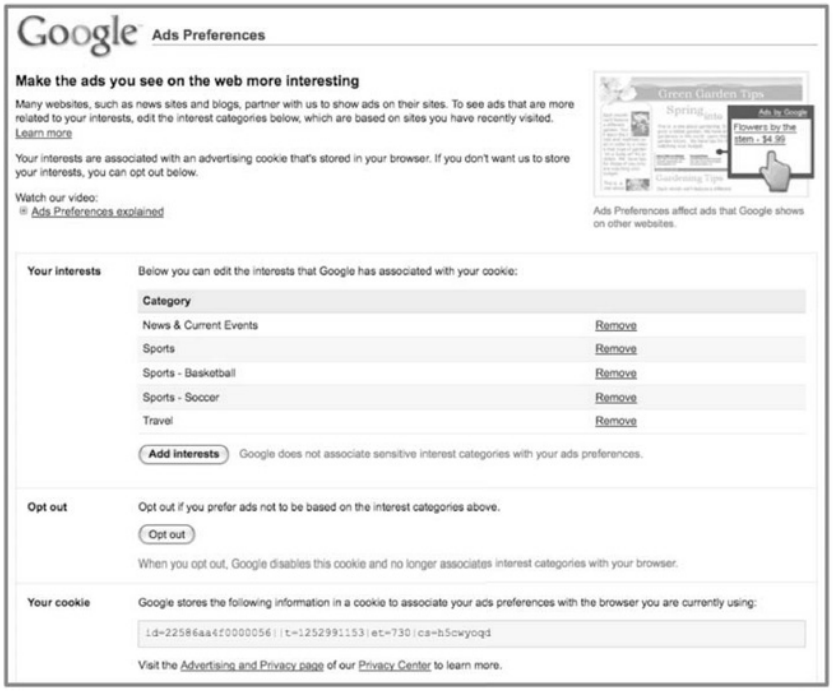


Fig. 2: Ads Preferences Manager

As an engineer, I like to evaluate things by looking at the data. In this case, we have begun to receive information about how users are interacting with the Ads Preferences Manager. While our data are preliminary, we have discovered that, for every user that has opted out, about four change their interest categories and remain opted in and about ten view their settings but do nothing. We take from this that online users appreciate transparency and control, and become more comfortable with data collection and use when we offer it on their terms and in full view.

Control Through Data Portability

Providing our users with control over their personal information must also mean giving them the ability to easily take their data with them if they decide to leave. Starting with our Gmail service and now covering more than 25 Google products where users create and store personal information, a cadre of Google engineers—self-named the "Data Liberation Front"—has built tools to allow our users to "liberate" their data if they choose to switch providers or to stop using one of our services. The critical insight of these engineers was to recognize that users should never feel stuck using a service because they are unable to easily retrieve the content they created and transfer it to another service or provider at no additional cost.

Every user of Gmail, Picasa, Reader, YouTube, Calendar, Apps for Business, Docs, iGoogle, Maps, and many other products already have access to data portability tools, and the team continues to work on additional products. Detailed information for users is available at *www.dataliberation.org*.

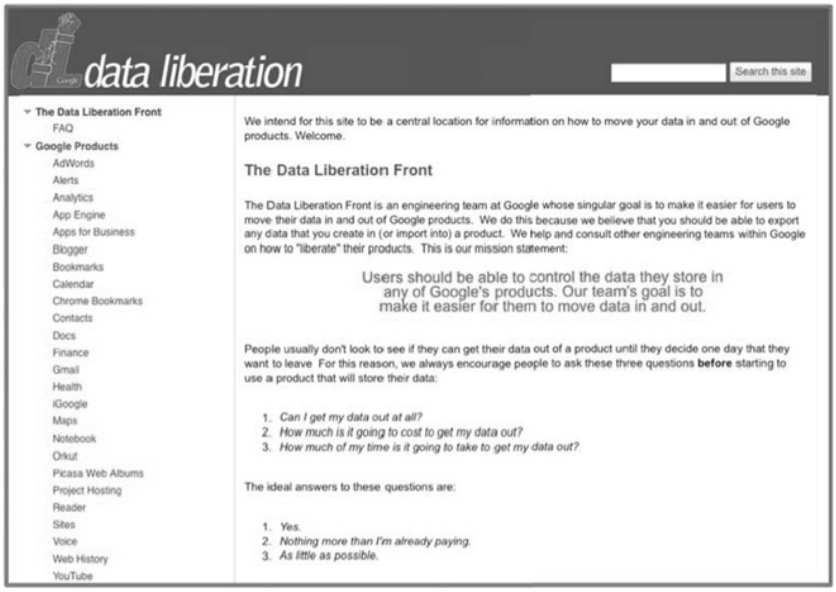


Fig. 3: Data Liberation Front

Data portability has benefits for our users and for Google. First, it keeps our product teams on their toes—they know just how easy it is for their users to move to a competitor's product, and understand that their success depends upon continuing to be responsive to privacy and product concerns and acting quickly to address them. Second, allowing our users the freedom to leave honors our commitment to put users in control.

In considering the testimony today and as the Committee develops its approach to consumer privacy, I urge you to consider the role that data portability can play in ensuring that consumer-facing businesses remain accountable for their privacy choices. Regulators should encourage this kind of "user empowerment by design" as an effective means of ensuring respect for user privacy without chilling innovation.

One-stop Shop for Transparency and Control: the Google Dashboard

Google developed the Google Dashboard (*www.google.com/dashboard*) to provide users with a one-stop, easy-to-use control panel to manage the use and storage of personal information associated with their Google accounts and products—from Gmail to Picasa to Search.

With the Dashboard, a user can see and edit the personally identifiable data stored with her individual Google account. A user also can change her password or password recovery options using Dashboard, and click to manage various products' settings, contacts stored with the account, or documents created or stored through Google Docs. Dashboard also lets a user manage chat data, by choosing whether or not to save it in her Google account.

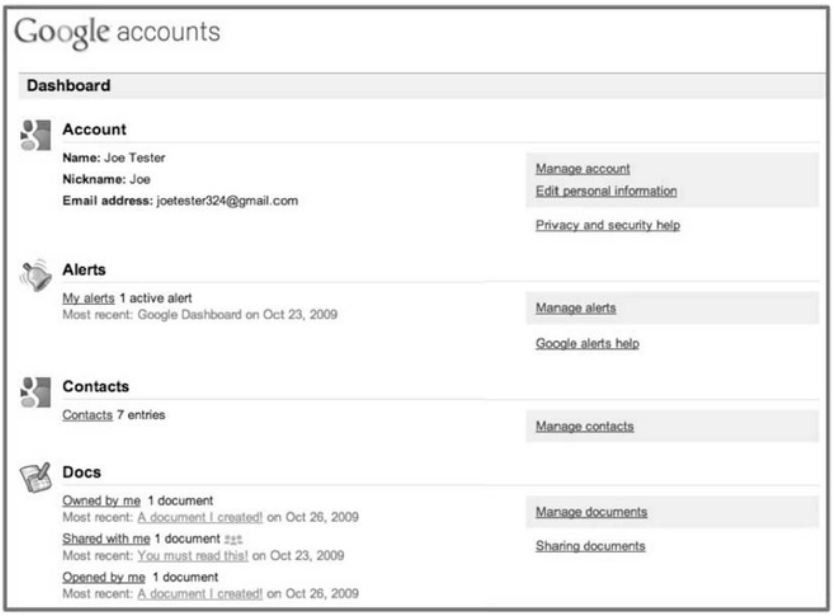


Fig. 4: Google Dashboard

Industry-leading Security: Encrypted Search and Gmail

Along with transparency and user control, good security is vital in maintaining user trust. Google faces complex security challenges while providing services to millions of people every day, and we have world-class engineers working at Google to help secure information. In fact, my own research background is in security. In a *1999 paper*, "Why Johnny Can't Encrypt," I argued that security tools must be simple and usable to be effective. Unfortunately, it is sometimes the case that security technology is so complicated that it isn't usable, and thus ineffective. I have continued that theme at Google, working to build user-friendly, simple security features into our products.

For example, Google recently became the first (and still only) major webmail provider to offer session-wide secure socket layer (SSL) encryption *by default*. Usually recognized by a web address starting with "https" or by a "lock" icon, SSL encryption is regularly used for online banking or transactions. As our Gmail lead engineer *wrote*:

> In 2008, we rolled out the option to *always use https*—encrypting your mail as it travels between your web browser and our servers. Using https helps protect data from being snooped by third parties. . . . We initially left the choice of using it up to you because there's a downside: https can make your mail slower since encrypted data doesn't travel across the web as quickly as unencrypted data. Over the last few months, we've been *researching the security/latency tradeoff* and decided that turning https on for everyone was the right thing to do.

We hope other companies will soon join our lead.

We also hope to see our competitors adopt another security tool we offer our users: encryption for search queries. Users can simply type in "*encrypted.google.com*" and encrypt their search queries and results. As we said in our *blog post* about encrypted search, "an encrypted connection is created between your browser and Google. This secured channel helps protect your search terms and your search results pages from being intercepted by a third party on your network."

And in March Google launched a system to notify users about suspicious activities associated with their accounts. By automatically matching a user's IP address to broad geographical locations, Google can help detect anomalous behavior, such as a log-in appearing to come from one continent only a few hours after the same account holder logged in from a different continent. Thus, someone whose Gmail ac-

count may have been compromised will be notified and given the opportunity to change her password, protecting her own account and her Gmail contacts.

Fig. 5: Recent Account Activity Warning

Similarly, we built Google Chrome with security in mind from the beginning, including features such as:

- Safe Browsing, which warns a user before he visits a site that it is suspected of phishing or containing malware;
- *Sandboxing*, which works automatically to help prevent web browser processes from harming one another or a user's computer, and
- Automatic updates that deliver security patches to users as quickly as possible.

Google also conducts extensive security research and provides free security resources to the broader Internet community. We make security tools available for free to webmasters to help them operate more secure sites, as well as to application developers to help them build more secure applications. For example, we *recently released* a tool called "skipfish" under an open source license to help identify web application vulnerabilities through fully automated, active security reconnaissance.

The Challenges of Designing for Privacy and Security

In addition to discussing Google's efforts to offer transparency, user control, and security, I want to also discuss just two of the many challenges I and others in similar roles face as we try to build privacy and security into innovative products. The first relates to data collection and use. The second involves how to best communicate to individuals how to manage their privacy.

Every day we receive information from our users' interaction with our products and services. That information may be in the form of an e-mail that we process, store, and protect in our Gmail product—or it could be generated by the interaction between a user's computer and our servers, such as a search query and the IP address associated with a specific computer or network of computers.

We are asked often why we retain this query and IP address data—which can be very sensitive even if it does not personally identify individuals. We certainly treat this data with strong security, and seek to build in transparency and user controls where appropriate—including tools like our Ads Preferences Manager. We also voluntarily anonymize IP addresses after 9 months.

But this data is actually tremendously helpful to us in improving our products and protecting our networks from hackers, spammers, and fraudsters. For example, bad actors continually seek to manipulate our search ranking, launch denial-of-service attacks, and scam our users via e-mail spam or malware. We use our log files to track, block, and keep ahead of the bad guys.

We also use information like IP addresses and search queries to develop products like Flu Trends (*www.google.com/flutrends*). A team of our engineers found that examining certain search terms on an aggregate basis can provide a good indicator of flu activity. Of course, not every person who searches for "flu" is actually sick, but a pattern emerges when many flu-related search queries are added together. By counting how often we see these search queries, we can estimate how much flu is circulating in different countries and regions around the world. Our *results* have been *published* in the journal *Nature*.

For epidemiologists, this is an exciting development, because early detection of a disease outbreak can reduce the number of people affected. If a new strain of influenza virus emerges under certain conditions, a pandemic could ensue with the potential to cause millions of deaths. Our up-to-date influenza estimates may enable public health officials and health professionals to better respond to seasonal epidemics and pandemics.

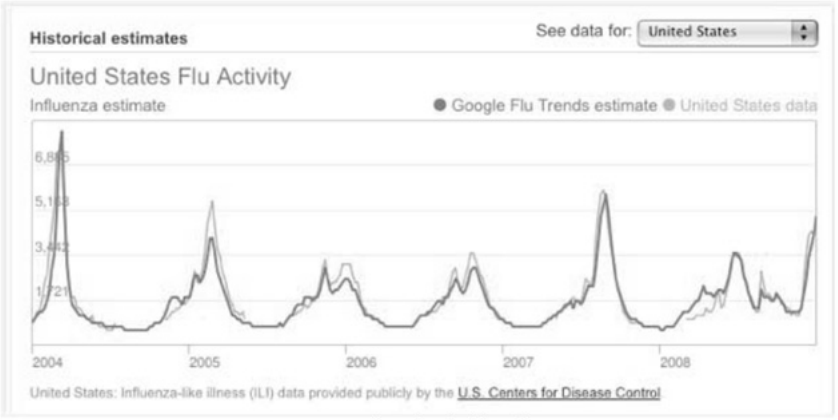


Fig. 6: Google Flu Trends

A second challenge is how to best communicate with our users about privacy.

At Google, we take great pride in our effort to provide our users with a better understanding of how we collect, use, and protect their data. For example, we have produced a series of short videos on privacy and made the videos available at Google.com and on YouTube. We also blog often about privacy in plain language aimed at educating our users. We believe that companies that interact and have relationships with consumers need to do more than simply provide and link to privacy policies; we all need to offer consumer-friendly materials in a variety of media to help users better understand how their information is collected and used, and what choices they have to protect their privacy.

We also believe in "transparency in context" so that consumers can benefit from privacy information *when and where they're actually using a product or service*, in addition to through a privacy policy. The concept of transparency in context underlies our desire to provide in-ad notice for interest-based ads. With such notice, consumers have easy access to both information and choice tools at the point of interaction with the relevant product.

There are times, of course, where we do not get it right on the first try. When we launched Google Buzz, a social networking service for sharing updates, photos, videos, and more, we heard from some users that they were unhappy. So our engineers worked around the clock and within 48 hours we had made significant product changes. Now, instead of automatically creating a list of followers, we suggest people for Buzz users to follow. We also made it easier for users to block others from following them. And we added a tab to Gmail settings making it easier to hide Buzz or disable it completely. Soon after, we sent out a confirmation page to early Buzz users giving them another opportunity to understand and *reconfirm their settings*.

These are the kind of updates and improvements we are making to all our products all the time, from Gmail to search to mobile, because control is what our users want and deserve—and what we want to provide.

Understanding the WiFi Incident

In those instances where mistakes occur, we try to understand and learn from our mistakes. I'd like to address the recent issue involving WiFi data in that context.

Several months ago, Google disclosed that we had mistakenly included code in the software on our Street View cars that collected samples of WiFi "payload data"—information sent over a WiFi network—from open (unencrypted) WiFi networks. Importantly, these samples of payload data have never been used in any Google product or service; nor do we intend to use them. If you would like more information about the facts and background of this incident, including the independent, third-party review of our software, my colleague Alan Eustace has *described it* on the Official Google Blog.

As Alan concluded, "We are profoundly sorry for this error and are determined to learn all the lessons we can from our mistake." While our legal team is still reviewing the matter, I can attest that it was not consistent with the value we place on the responsible handling of personal data. Google is taking the review of this matter very seriously and we will report back with the changes we'll make to prevent such a thing from happening in the future.

The incident also reaffirms to us the importance of transparency. Data collection and use practices should be disclosed, and in plain language. When mistakes occur, companies ought to continue providing that transparency—as Google did here even in the absence of any breach of personal data—by quickly and simply disclosing what occurred, any risk posed to users, and how users can mitigate that risk.

How Congress Can Encourage Responsible Privacy Practices and Build Trust

Congress has a vital role to play in encouraging responsible privacy and security practices, both by bringing attention to these issues and through appropriate legislation. Google supports the development of comprehensive, baseline privacy legislation that can ensure broad-based user trust and that will support continued innovation and serve the privacy interests of consumers.

I am a scientist and engineer, not a lawyer, but I have some basic thoughts about what good policy needs to accomplish in this area.

- *Even-handed application.* A pro-innovation privacy framework must apply even-handedly to all personal data regardless of source or means of collection. Thus, offline data collection and processing should, where reasonable, involve similar data protection obligations.
- *Recognition of benefits and costs.* As with any regulatory policy, it is appropriate to examine the benefits and costs of legislating in this area, including explicit attention to actual harm and compliance costs.
- *Security requirements and breach notification.* We pride ourselves at Google for industry-leading security features, including the use of encryption for our search and Gmail services I discussed. A thorough privacy framework should promote uniform, reasonable security principles, including data breach notification procedures.
- *Clear process for compelled access.* The U.S. law governing government access to stored communications is outdated and out of step with what is reasonably expected by those who use cloud computing services. The problems in the law threaten the growth, adoption, and innovation of cloud technologies without a corresponding benefit. As part of the *Digital Due Process coalition*, we are working to address this issue. The Committee can play an important role in encouraging clear rules for compelled access to user data.
- *Consistency across jurisdictions.* Generally, Internet users neither expect nor want different baseline privacy rules based on the local jurisdiction in which they or the provider reside. Moreover, in many instances, strict compliance with differing state or national privacy protocols would actually diminish consumer privacy, since it would require Internet companies to know where consumers are located at any given time.

Any new privacy law must also offer baseline protections on which providers can innovate. A pro-innovation privacy framework offers providers the flexibility to both develop self-regulatory structures and individually innovate in privacy practices and tools. The advertising industry and online publisher efforts to *develop self-regulatory rules* for interest-based advertising, for example, are a strong example of the need for and utility of industry-driven efforts. As I have discussed, Google has been a leader in developing innovative privacy tools.

Continued innovation in the privacy space is vital for users. Unfortunately, compliance-based or overly complex rules can lock in a specific privacy model that may quickly become obsolete or insufficient due to the speed with which Internet services evolve. A principles-based model encourages innovation and competition in privacy tools.

A baseline framework needs to encourage the development of innovative tools like the ones I've described. We believe that stable, baseline principles set by law can permit flexible, adaptive structures to develop on top—much like the stable protocols and standards at the physical and network layers of the Internet allow flexible and innovative development at the content and application layers. With comprehensive, baseline privacy legislation establishing ground rules for all entities, self-regulatory standards and best practices of responsible industry actors will evolve over time. On top of that structure, individual companies will be free (and encouraged) to create innovative privacy tools and policies rather than stick with potentially outdated compliance structures.

Conclusion

Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee, thank you for inviting me to testify today. We at Google appreciate the op-

portunity to discuss online privacy and how our company has helped lead in the effort to protect our users by providing them with transparency, user control, and security.

I look forward to answering any questions you might have about our efforts, and Google looks forward to working with members of the Committee and others in the development of better privacy protections.

Thank you.

The CHAIRMAN. Thank you, Dr. Whitten.

Now Mr. Jim Harper, Director of Information Policy Studies at The Cato Institute.

STATEMENT OF JIM HARPER, DIRECTOR OF INFORMATION POLICY STUDIES, THE CATO INSTITUTE

Mr. HARPER. Thank you, Mr. Chairman. Good afternoon. Thanks for inviting me to testify today. And I definitely appreciate that you're educating the Committee and the public about consumer online privacy.

My 21-page single-spaced written testimony——

[Laughter.]

Mr. HARPER.—is only a brief glance at the many issues that are involved in privacy regulation and fair information practices. I suspect that the much more useful 1-page executive summary is what'll benefit you and your staff in your early examination of the issue.

What it says is that privacy is a complicated human interest. When people talk about privacy, they may mean desire for fair treatment, they may mean security from identity fraud and other crimes, they may mean distaste for being marketed to as objects of crass commercialism, and they may mean something more like liberty or autonomy. I think the strongest sense of the word "privacy" refers to control of personal information. That is, having the ability to selectively reveal things about yourself so that you can craft the image you portray to all the different communities that you interact with in your life.

As we've seen in discussion here today, the online environment is new and different. Many people literally don't know how to control information about themselves. Other technologists with me on the panel today are doing good work, I think, to try to rectify that, but it won't be easy.

I may play "skunk at the garden party" when I say that I have doubts about the capacity of fair information practices and regulatory solutions to solve these problems and deliver privacy. Fair information practices have a long history, nearly 40 years, and there are many good practices, described by fair information practices, that many companies should probably do. But, just like there are many different senses of privacy, there are many different data practices that matter in different degrees at different times. So, blanket use of fair information practices is probably inappropriate and unhelpful.

In my written testimony I focused heavily on notice and the failure of notice, really, over the last decade, to deliver privacy like many thought it would, 10 years ago. I think the short-notice project is wonderful and fine, but I don't hold out much hope that it will lead to an upwelling of privacy awareness, like I think we all would like to have.

I also emphasize how changing business models and changing Internet protocols make it difficult to regulate, prospectively, in ways that'll work. Regulations may prevent new protocols—even worse—and new ways of interacting online from coming into existence. This would be a pity, because it would deny all of us the next generation of Internet-enabled innovations.

It would also be a pity if privacy regulation were to lock in competitive advantages for the companies that are leading the pack today. For all the good they do consumers, the companies represented by my copanelists at the table, I think, should always be met by searing competition. And companies can use the legislative and regulatory process to lock out competition, foreclose new business models as privacy-problematic.

Before I conclude, I want to change hats, really briefly, and talk about an issue that I know is on the mind of many people, and that's targeted advertising. Targeted advertising is sensitive, I think, because it represents a loss of control over personal information, like we've talked about. It also objectifies consumers, as such, rather than treating them as human beings who laugh and cry and aspire and get frustrated and fall in love. I think I understand that concern, but it doesn't motivate me as a privacy advocate.

But, what I want to talk about is my experience as the operator of a small website. As I noted in my written testimony, I run a website called *washingtonwatch.com.* It had about 1.6 million visitors last year, which is pretty good. One bill has 150,000 comments, I'll tell you, so I'm quite aware of the passions that unemployment compensation generates. I run the site in my spare time, and I've built it with my own funds, over several years. I'm fond of joking that it's the reason why I don't have a boat in my driveway. In fact, it might be the reason why I don't have a driveway.

I run Google ads to help defray the costs. AdSense is a pretty good product, though I am looking around. Amazon has a pretty cool thing going right now, called Omakase.

Here's the thing. I have tons of features that I want to add to *washingtonwatch.com,* and I decide to add new features when I feel like I have the money to do it. OK? I pay my Web developers about twice what I make per hour to work on the site. Of course, my sob story doesn't matter, but I probably stand in the shoes of many small Website operators and bloggers who choose whether they're going to add more content and more features based on whether they can afford it.

Targeted advertising is a way for sites, small and large, to support themselves better so that they can do more cool stuff for American citizens and consumers. Targeted ads, I think it's clear from economic study, are more valuable than contextual ads, more valuable that noncontextual, just blanket advertising.

My point is only this: Curtailing targeted advertising in the name of privacy involves tradeoffs with other important consumer issues. And these things are all important to discuss.

Thanks, again, so much for inviting me to testify today. Happy to answer your questions.

[The prepared statement of Mr. Harper follows:]

PREPARED STATEMENT OF JIM HARPER, DIRECTOR OF INFORMATION POLICY STUDIES, THE CATO INSTITUTE

Executive Summary

Privacy is a complicated human interest. People use the word "privacy" to refer to many different things, but its strongest sense is control of personal information, which exists when people have legal power to control information and when they exercise that control consistent with their interests and values.

Direct privacy legislation or regulation is unlikely to improve on the status quo. Over decades, a batch of policies referred to as "fair information practices" have failed to take hold because of their complexity and internal inconsistencies.

Even modest regulation like mandated privacy notices have not produced meaningful improvements in privacy. Consumers generally do not read privacy policies and they either do not consider privacy much of the time, or they value other things more than privacy when they interact online.

The online medium will take other forms with changing times, and regulations aimed at an Internet dominated by the World Wide Web will not work with future uses of the Internet. Privacy regulations that work "too well" may make consumers worse off overall, not only by limiting their access to content, but by giving supernormal profits to today's leading Internet companies and by discouraging consumer-friendly innovations.

The "online" and "offline" worlds are collapsing rapidly together, and consumers do not have separate privacy interests for one and the other. Likewise, people do not have privacy interests in their roles as consumers that are separate from their interests as citizens. If the Federal Government is going to work on privacy protection, it should start by getting its own privacy house in order.

Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee, thank you for inviting me to address your hearing on "Consumer Online Privacy."

My name is Jim Harper, and I am Director of Information Policy Studies at the Cato Institute. In that role, I study and write about the difficult problems of adapting law and policy to the challenges of the information age. Cato is a market liberal, or libertarian, think-tank, and I pay special attention to preserving and restoring our Nation's founding traditions of individual liberty, limited government, free markets, peace, and the rule of law.

My primary focus is on privacy and civil liberties, and I serve as an advisor to the Department of Homeland Security as a member of its Data Integrity and Privacy Advisory Committee. I am not a technologist, but a lawyer familiar with technology issues. As a former committee counsel in both the House and Senate, I understand lawmaking and regulatory processes related to technology and privacy. I have maintained a website called *Privacilla.org* since 2000,[1] cataloguing many dimensions of the privacy issue, and I also maintain an online Federal legislative resource called *WashingtonWatch.com,*[2] which has had over 1.6 million visitors in the last year.

What is Privacy?

Your hearing to explore consumer online privacy is welcome. There are many dimensions to privacy, and it is wise to examine all of them, making yourselves aware of the plethora of issues and considerations before turning to legislation or regulation.

People use the word "privacy" to describe many concerns in the modern world, including fairness, personal security, seclusion, and autonomy or liberty. Given all those salutary meanings, everyone wants "privacy," of course. Few concepts have been discussed so much without ever being solidly defined. But confusion about the meaning of the word makes legislation or regulation aimed at privacy difficult.

"Privacy" sometimes refers to the interest violated when a person's sense of seclusion or repose is upended. Telephone calls during the dinner hour,[3] for example,

---

[1] *http://www.privacilla.org*

[2] *http://www.washingtonwatch.com* Disclosure: *WashingtonWatch.com* defrays some costs of its otherwise money-losing operation by running Google AdSense ads.

[3] *See* Federal Trade Commission, "Unwanted Telephone Marketing Calls" web page *http://www.fcc.gov/cgb/consumerfacts/tcpa.html*.

spam e-mails,[4] and—historically—the quartering of troops in private homes[5] undermine privacy and the vaunted "right to be let alone."[6]

For some, it is marketing that offends privacy—or at least targeted marketing based on demographic or specific information about consumers. Many people feel something intrinsic to individual personality is under attack when people are categorized, labeled, filed, and objectified for commerce based on data about them.

This is particularly true when incomplete data fails to paint an accurate picture. The worst denial of personality occurs in the marketing area when data and logic get it wrong, serving inappropriate marketing communications to hapless consumers. A couple who recently lost their baby receives a promotion for diapers or children's toys, for example. Or mail for a deceased parent continues coming long after his or her passing. In the informal sector, communities sometimes attack individuals because of the inaccurate picture gossip paints on the powerful medium of the Internet.[7]

The "privacy" damage is tangible when credit bureaus and other reputation providers paint an incomplete or wrong picture. Employers and credit issuers harm individual consumers when they deny people work or credit based on bad data or bad decision rules.[8]

Other kinds of "privacy" violations occur when criminals acquire personal information and use it for their malign purposes. The scourge of identity theft is a well known "privacy" problem. Drivers Privacy Protection Acts[9] passed in many state legislatures and in the U.S. Congress after actress Rebecca Schaeffer was murdered in 1989. Her stalker got her residence information from the California Department of Motor Vehicles. In a similar notable incident a decade later, Vermont murderer Liam Youens used a data broker to gather information as part of an Internet-advertised obsession with the young woman he killed.[10]

"Privacy" is also under fire when information demands stand between people and their freedom to do as they please. Why on earth should a person share a phone number with a technology retailer when he or she buys batteries? The U.S. Department of Homeland Security has worked assiduously in what is now called the "Secure Flight" program to condition air travel on the provision of accurate identity information to the government, raising the privacy costs of otherwise free movement.

Laws banning or limiting medical procedures dealing with reproduction offend "privacy" in another sense of the word.[11] There are a lot of privacy problems out there, and many of them blend together.

Privacy as Control of Personal Information

The strongest and most relevant sense of the word "privacy," which I will focus on here, though, is its "control" sense—privacy as control over personal information. Privacy in this sense is threatened by the Internet, which is an unusual new medium for many people over the age of eighteen.

In his seminal 1967 book *Privacy and Freedom,* Alan Westin characterized privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[12] A more precise, legalistic definition of privacy in the control sense is: the

---

[4] The CAN–SPAM Act of 2003 (15 U.S.C. 7701, et seq., Public Law No. 108–187) was intended to remedy the problem of spam, but it remains a huge amount of the SMTP traffic on the Internet. *See* Jim Harper, "CAN–SPAM Didn't—Not By a Long Shot," Cato@Liberty (Nov. 6, 2006) *http://www.cato-atliberty.org/2006/11/06/can-spam-didnt-not-by-a-long-shot/*.

[5] *See* U.S. Const. amend. III (barring quartering of troops in peacetime).

[6] *Olmstead* v. *United States*, 277 U.S. 438 (1928) (Brandeis, J, dissenting). Unfortunately, the *Olmstead* case was not about "seclusion" but control of information traveling by wire.

[7] In his book, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET, George Washington University Law School professor Daniel Solove details the story of "Dog Poop Girl," for example, who was selected for worldwide ridicule when a photo of her failing to clean up after her pooch was uploaded and disseminated over the Internet. DANIEL SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET (New Haven: Yale University Press, 2007) pp. 1–4.

[8] Congress passed the Fair Credit Reporting Act (codified at 15 U.S.C. § 1681 et seq.) in 1970 intending to produce fairness in the credit reporting world, which is still an area of difficulty for consumers.

[9] The Federal Drivers Privacy Protection Act, Public Law No. 103–322, amended by Public Law 106–69, prohibits the release or use by any State DMV (or officer, employee, or contractor thereof) of personal information about an individual obtained by the department in connection with a motor vehicle record. It sets penalties for violations and makes violators liable on a civil action to the individual to whom the released information pertains.

[10] *See Remsburg* v. *Docusearch, Inc.* (N.H. 2003) *http://www.courts.state.nh.us/supreme/opinions/2003/remsb017.htm*.

[11] *See Griswold* v. *Connecticut*, 381 U.S. 479 (1965); *Roe* v. *Wade*, 410 U.S. 113 (1973).

[12] ALAN F. WESTIN, PRIVACY AND FREEDOM, p. 7 (New York: Atheneum 1967).

subjective condition people experience when they have power to control information about themselves and when they have exercised that power consistent with their interests and values.[13] The "control" sense of privacy alone has many nuances, and I will parse them here briefly.

Importantly, privacy is a subjective condition. It is individual and personal. One person cannot decide for another what his or her sense of privacy is or should be.

To illustrate this, one has only to make a few comparisons: Some Americans are very reluctant to share their political beliefs, refusing to divulge any of their leanings or the votes they have cast. They keep their politics private. Their neighbors may post yard signs, wear brightly colored pins, and go door-to-door to show affiliation with a political party or candidate. The latter have a sense of privacy that does not require withholding information about their politics.

Health information is often deemed intensely private. Many people closely guard it, sharing it only with doctors, close relatives, and loved ones. Others consent to have their conditions, surgeries, and treatments broadcast on national television and the Internet to help others in the same situation. More commonly, they relish the attention, flowers, and cards they receive when an illness or injury is publicized. Privacy varies in thousands of ways from individual to individual and from circumstance to circumstance.

An important conclusion flows from the observation that privacy is subjective: government regulation in the name of privacy can be based only on guesses about what "privacy" should look like. Such rules can only ape the privacy-protecting decisions that millions of consumers make in billions of daily actions, inactions, transactions, and refusals. Americans make their highly individual privacy judgments based on culture, upbringing, experience, and the individualized costs and benefits of interacting and sharing information.

The best way to protect true privacy is to leave decisions about how personal information is used to the people affected. Regulatory mandates that take decision-making power away from people will prevent them striking the balances that make them the best off they can be. Sometimes it is entirely rational and sensible to share information.

> Privacy has to do with control of information and its effects on people. To illustrate the complexity of privacy when technology is involved, read "Privacy Advocates Who Don't Understand Privacy" at Appendix I.

At its heart, privacy is a product of autonomy and personal responsibility. Only empowered, knowledgeable citizens can formulate and protect true privacy for themselves, just as they individually pursue other subjective conditions, like happiness, piety, or success.

The Role of Law

The legal environment determines whether people have the power to control information about themselves. Law has dual, conflicting effects on privacy: Much law protects the privacy-enhancing decisions people make. Other laws undermine individuals' power to control information.

Various laws foster privacy by enforcing individuals' privacy-protecting decisions. Contract law, for example, allows consumers to enter into enforceable agreements that restrict the sharing of information involved in, or derived from, transactions.

Thanks to contract, one person may buy foot powder from another and elicit as part of the deal an enforceable promise never to tell another soul about the purchase. In addition to explicit terms, privacy-protecting confidentiality has long been an implied term in many contracts for professional and fiduciary services, like law,

[13] *See generally*, Jim Harper, "Understanding Privacy—and the Real Threats to It," Cato Policy Analysis No. 520 (Aug. 4, 2004) *http://www.cato.org/pub__display.php?pub__id=1652*.

medicine, and financial services. Alas, legislation and regulation of recent vintage have undermined those protections.[14]

Many laws protect privacy in other areas. Real property law and the law of trespass mean that people have legal backing when they retreat into their homes, close their doors, and pull their curtains to prevent others from seeing what goes on within. The law of battery means that people may put on clothes and have all the assurance law can give that others will not remove their clothing and reveal the appearance of their bodies without permission.

Whereas most laws protect privacy indirectly, a body of U.S. state law protects privacy directly. The privacy torts provide baseline protection for privacy by giving a cause of action to anyone whose privacy is invaded in any of four ways.[15]

The four privacy causes of action, available in nearly every state, are:

- Intrusion upon seclusion or solitude, or into private affairs;
- Public disclosure of embarrassing private facts;
- Publicity that places a person in a false light in the public eye; and
- Appropriation of one's name or likeness.

While those torts do not mesh cleanly with privacy as defined here, they are established, baseline, privacy-protecting law.

Law is essential for protecting privacy, but much legislation plays a significant role in undermining privacy. Dozens of regulatory, tax, and entitlement programs deprive citizens of the ability to shield information from others. You need only look at the Internal Revenue Service's Form 1040 and related tax forms to see that.

Consumer Knowledge and Choice

I wrote above about the role of personal responsibility in privacy protection. Perhaps the most important, but elusive, part of privacy protection is consumers' exercise of power over information about themselves consistent with their interests and values. This requires consumers and citizens to be aware of the effects their behavior will have on exposure of information about them.

Technology and the world of commerce are rapidly changing, and personal information is both ubiquitous and mercurial. Unfortunately, there is no horn that sounds when consumers are sufficiently aware, or when their preferences are being honored. But study of other, more familiar, circumstances reveals how individuals have traditionally protected privacy.

Consumers' privacy preferences are unpredictable and changing. To see an illustration of this, read about Facebook's "News Feed" in Appendix II.

Consider privacy protection in the physical world. For millennia, humans have accommodated themselves to the fact that personal information travels through space

[14] The Gramm-Leach-Bliley Act and Federal regulations under the Health Insurance Portability and Accountability Act institutionalized sharing of personal information with government authorities and various "approved" institutions. See 15 U.S.C. §§ 6802(e)(5)&(8); various subsections of 45 C.F.R. 164.512.

[15] *Privacilla.org,* "The Privacy Torts: How U.S. State Law Quietly Leads the Way in Privacy Protection," (July 2002) *http://www.privacilla.org/releases/Torts__Report.html.*

and air. Without understanding how photons work, people know that hiding the appearance of their bodies requires them to put on clothes. Without understanding sound waves, people know that keeping what they say from others requires them to lower their voices.

From birth, humans train to protect privacy in the "natural" environment. Over millions of years, humans, animals, and even plants have developed elaborate rules and rituals of information sharing and information hiding based on the media of light and sound.

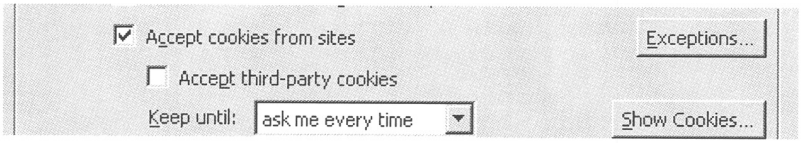
Tinkering with these rules and rituals today would be absurd. Imagine, for instance, a privacy law that made it illegal to observe and talk about a person who appeared naked in public without giving the nudist a privacy notice and the opportunity to object. People who lacked the responsibility to put on clothes might be able to sue people careless enough to look at them and recount what they saw. A rule like that would be ridiculous.

The correct approach is for consumers to be educated about what they reveal when they interact online and in business so that they know to wear the electronic and commercial equivalents of clothing.

Of all the online privacy concerns, perhaps the most fretting has been done about "behavioral advertising"—sometimes referred to as "psychographic profiling" to get us really worked up. What is truly shocking about this problem, though, is that the remedy for most of it is so utterly simple: exercising control over the cookies in one's browser.

Cookies are small text files that a website will ask to place in the memory of computers that visit it. Many cookies have distinct strings of characters in them that allow the website to "recognize" the computer when it visits the site again. When a single domain places content across the web as a "third party"—something many ad networks do—it can recognize the same computer many places and gain a sense of the interests of the user.

The solution is cookie control: In the major browsers (Firefox and Internet Explorer), one must simply go to the "Tools" pull-down menu, select "Options," then click on the "Privacy" tab to customize one's cookie settings. In Firefox, one can decline to accept all third-party cookies (shown inset), neutering the cookie-based data collection done by ad networks. In Internet Explorer, one can block all cookies, block all third-party cookies, or even choose to be prompted each time a cookie is offered.[16]



Again, consumers educated about what they reveal when they interact online can make decisions about how to behave that will protect privacy much better—in all online contexts—than consumers unaware of how the world around them works.

Can Direct Regulation Protect Privacy Better?

Above, I wrote about how law protects people's privacy-protecting decisions. This unfortunately leaves them with the responsibility of making those decisions. Naturally, most privacy advocates—myself included—believe that people do not do enough to protect their privacy. Consciously or not, people seem to prioritize the short-term benefits of sharing personal information over the long-term costs to their privacy.

This poses the question: Can direct regulation protect consumers privacy better than they can protect themselves?

There is a decades-long history behind principles aimed at protect privacy and related interests, principles that are often put forward as a framework for legislative or regulatory directives.

In the early 1970s, a group called "The Secretary's Advisory Committee on Automated Personal Data Systems" within the Department of Health, Education, and Welfare did an important study of record-keeping practices in the computer age. The

[16] These methods do not take care of an emerging tracker known as "Flash cookies" which must be disabled another way, but consumers aware of their ability and responsibility to control cookies can easily meet the growth of Flash cookies. *See* "Flash Player Help" web page, Global Privacy Settings panel, *http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager02.html*.

intellectual content of its report, commonly known as the "HEW Report,"[17] formed much of the basis of the Privacy Act of 1974. The report dealt extensively with the use of the Social Security Number as the issues stood at that time.

The HEW report advocated the following "fair information practices":

- There must be no personal-data record-keeping systems whose very existence is secret.
- There must be a way for an individual, to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

These things sound wonderful in the abstract, but their relevance, worthiness, and cost-justifications vary widely from circumstance to circumstance.

In 1980, the Organization for Economic Cooperation and Development (OECD)[18] issued similar, if more detailed guidelines. The OECD Guidelines involve eight principles, which in different variations are often touted as "fair information practices" or "fair information practice principles."

They include a "Collection Limitation Principle," a "Data Quality Principle," a "Purpose Specification Principle," a "Use Limitation Principle," a "Security Safeguards Principle," an "Openness Principle," an "Individual Participation Principle," and an "Accountability Principle." The full OECD principles, in their sprawling glory, are reproduced in a footnote below.[19]

---

[17] "Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems," Department of Health, Education, and Welfare [now Department of Health and Human Services] (July, 1973) *http://www.aspe.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm*.

[18] The OECD consists of bureaucrats from 29 countries that work to coordinate policies with the nominal aim of fostering international trade. The United States is a member of the OECD and the largest funders of its $424 million dollar 2010 budget. See Organization for Economic Cooperation and Development, "Member Countries' Budget Contributions for 2010" web page *http://www.oecd.org/document/14/0,3343,en_2649_201185_31420750_1_1_1_1,00.html*.

[19] 1. Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, compete and kept up-to-date.

3. Purpose Specification Principle: The purposes for which personal data are collected should be specified not later than at the time of collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Principle 3 except:

—with the consent of the data subject; or
—by the authority of law.

5. Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

6. Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual Participation Principle: An individual should have the right:

—(a) to obtain from the data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
—(b) to have communicated to him, data relating to him
—within a reasonable time;
—at a charge, if any, that is not excessive;
—in a reasonable manner; and
—in a form that is readily intelligible to him;
—(c) to be given reasons if a request made under sub-paragraphs (a) and (b) is denied, and to be able to challenge such denial; and

In a 2000 report, the Federal Trade Commission came out with a relatively briefer list of "fair information practices" (notice, choice, access, and security) and asked Congress for authority to impose them on the businesses of the country,[20] even though a committee convened by the FTC could not reconcile the inherent tensions between access and security.[21] Congress declined to take the FTC's advice.

These examples illustrate one of the problems with the idea of "baseline privacy regulation" for the Internet that has been a consistent call of many for over a decade. There are many good ideas and good practices described in the HEW Report, the OECD Guidelines, and in various other iterations of "fair information practices," but tensions among the principles and variations in their applicability to different circumstances make "FIPs" a poor guide for smart legislating.

"Fair information practices" remain largely aspirational after nearly 40 years, and where they have been implemented, privacy has not blossomed. The principal example is the Privacy Act of 1974, which has done little to give American citizens control over information the government collects. It is shot through with exceptions, and it is largely a paper tiger.

The Fair Credit Reporting Act has guided the development of the credit reporting industry for four decades, while insulating credit bureaus from state tort laws. During that period, the industry has become highly cartelized, consisting of three players (as discussed below, a typical consequence of regulatory barriers to entry). It has failed to innovate and become the reputation and identity service that the world of e-commerce could use. And—most importantly for these purposes—credit reporting is a consumer-unfriendly industry. Rather than working with consumers to develop mutually beneficial personal data repositories, the credit reporting industry serves its financial industry partners first, Federal regulators second, and consumers as a rather distant afterthought.

The privacy regulations implemented under the Health Insurance Portability and Accountability Act are sometimes touted as reflecting "fair information practices." (With their breadth, any good data practice is arguably a FIP.) But health privacy has not materialized since Congress shrugged its shoulders and handed the privacy problem to the Department of Health and Human Services.[22] Pre-HIPAA studies showing that patients sometimes avoided treatment due to privacy worries have not been matched by post-HIPAA studies showing that consumers confident of health privacy are getting medical care they would not have gotten.

Fair information practices are widely touted as models for direct regulation that would protect privacy. But the examples we have of FIP-style laws and regulations have not delivered privacy. Privacy protection is hard, and it is not amenable to top-down solutions.

Keeping it Simple: What About Privacy Notice?

If the full suite of "fair information practices" is too intricate and internally inconsistent to produce a flowering of privacy across the land, perhaps some minimal privacy regulation would move the ball in the right direction. Mandated privacy notices are widely regarded as a step that would put consumers in a position to protect privacy themselves.

One would think. But they haven't.

A decade ago, market pressure spurred commercial websites to adopt and publish privacy policies. The FTC found in its 2000 report that 100 percent of the most popular sites on the web and 88 percent of randomly sampled sites had privacy disclosures of some kind.[23] This was in the absence of any regulation requiring notice; it was simply the product of market-based consensus that privacy notice was an appropriate business practice.

However, over the ensuing decade it has become clear that privacy notices do not materially improve consumers' privacy practices. The Federal Trade Commission,

---

—(d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

8. Accountability Principle: A data controller should be accountable for complying with measures which give effect to the principles stated above.

[20] Federal Trade Commission, "Privacy Online: Fair Information Practices in the Electronic Marketplace," (May 2000) *http://www.ftc.gov/reports/privacy2000/privacy2000.pdf*.

[21] *See* FTC Advisory Committee on Online Access and Security, "Final Report of the Federal Trade Commission Advisory Committee on Online Access and Security" (May 15, 2000) *http://www.ftc.gov/acoas/*.

[22] *See Privacilla.org,* "Health Privacy in the Hands of Government: The HIPAA Privacy Regulation—Troubled Process, Troubling Results" (April, 2003) *http://www.privacilla.org/releases/HIPAA_Report.pdf*.

[23] *See* Federal Trade Commission, "Privacy Online: Fair Information Practices in the Electronic Marketplace," Appendix C, Table 2A (May 2000) *http://www.ftc.gov/reports/privacy2000/privacy2000.pdf*.

other agencies, researchers like Lorrie Faith Cranor at Carnegie Mellon University's "CUPS" laboratory,[24] and others are diligently pursuing strategies to make notices effective at communicating privacy information to consumers in the hope that they will act on that information. But none has yet borne fruit.

The FTC and seven other regulators recently revealed a new, "short" financial privacy notice (required annually of financial services providers by the Gramm-Leach-Bliley Act) that they say "will make it easier for consumers to understand how financial institutions collect and share information about consumers."[25] Perhaps privacy awareness will flourish in the financial services area under this new regime, validating the widely derided privacy notices that clutter Americans' mailboxes. More likely, artificial "notice" will continue to lose currency as a tool for generating consumer focus on privacy.

Nutrition labels, the beloved model for privacy notices, have failed to stem the tide of fat washing over Americans' waistlines. Consumer behavior is difficult to control, as it should be in a free country.

Notice has other challenges. If it ever was, the "online" environment is no longer confined to a series of web pages, of which one could contain a universal privacy policy. The Internet is amenable to endless new protocols and forms of communication, which may defy the idea that there is somewhere for a notice to be located.

Even the growth of handheld devices—an incremental step in comparison to what may come in the future—challenges the idea of notice. Given the very small screen space of many devices, where is a notice to be located? And where is a notice to be located when there isn't a hypertext "link" structure to follow?

A hint of how unsuited privacy notices are to the future of the Internet lies in a dust-up about Google's privacy notice that occurred in mid–2008. A California law passed in 2003 requires websites to have privacy policies linked to from their home pages.[26] At some point, privacy advocates noticed that Google did not have such a link. Access to Google's industry-leading "Privacy Center" was accessible by doing a search on any number of terms or phrases, such as: *What is Google's privacy policy?*

Google, after all, is a search engine. In fact, it is the search engine that augured the decline of the Internet "portal" in favor of more fluid, search-based entrée to the web. Yet the California law requires a portal-style link, something that Google agonized over, being very proud of their very clean home page.[27] Google now has a privacy link on its home page. It has cured its online paperwork violation.

As this story illustrates, Americans are not going on the web through portals any more. Americans are not going "online" sitting at computers looking at web pages any more. There is no end to the protocols that people may use to communicate on the Internet, and a notice regime designed for the World Wide Web so popular in the decade just past will fail to reach people in the decades to come.

What Does "Online" Mean Anyway? And Why Is It Important?

It is important to consider changes in technology of a different kind, particularly the vanishing border between "online" and "offline." As I deliver my oral testimony to the Committee today, for example, I will be nominally "offline." However, audio and video of my presentation may be streamed live over the Internet or recorded and posted on the Committee's website or elsewhere. Reporters and researchers may take snippets of what I say and weave them into their work, posting those works online.

The phone in my pocket will be signaling its whereabouts (and inferentially mine) to nearby cell towers. Video of me entering, walking around inside, and leaving the Russell building may be captured and stored by the Capitol Police. Should the need arise, they may move this video into permanent storage.

There are privacy consequences from all these things. More than others, I suppose, I knowingly and willingly encounter privacy loss in order to be here and speak to you.

---

[24] *http://cups.cs.cmu.edu/*.

[25] Press release, "Federal Regulators Issue Final Model Privacy Notice Form" (Nov. 17, 2009) *http://www.cftc.gov/ucm/groups/public/@newsroom/documents/pressrelease/opafinalprivacynoticeform.pdf*.

[26] *See* Jim Harper, "Google Fakes Compliance with Privacy Law. Obscure Blogger Demands Investigation. Developing . . ." *TechLiberation.com* (July 4, 2008) *http://techliberation.com/2008/07/04/google-fakes-compliance-with-privacy-law-obscure-bloggerdemands-investigation-developing/*.

[27] *See* Marissa Meyer, "What comes next in this series? 13, 33, 53, 61, 37, 28 . . ." The Official Google Blog (July 3, 2008) *http://googleblog.blogspot.com/2008/07/what-comes-next-in-this-series–13–33–53.html*.

But what is the difference between the privacy consequences of this "offline" behavior and "online" behavior. Why should special privacy protections kick in when one formally sits down in front of a computer or uses a handheld device to go "online" if so much of "offline" life means the same thing?

The distinction between online and offline is blurring, and legislation or regulation aimed at protecting consumers "online" could create strange imbalances between different spheres of life. Consumers do not have a set of privacy interests that applies to the "online" world and another set that applies "offline."

To address online privacy alone is to miss the mark. This is not to say that the flesh-andblood world should have privacy regulations like those that have been dreamed up for the Internet. Rather, privacy on the Internet might better be produced the way it is in the "real" world, by people aware of the consequences of their behavior acting in their own best interests.

Privacy Regulation Might Also Work "Too Well"

Consumer privacy legislation and regulation might fail because they miss new protocols or technologies, uses of the Internet that are not web-based, for example. But there is an equally plausible likelihood that privacy regulation works too well, in a couple of different senses.

Privacy regulation that works "too well" would give people more privacy than is optimal, making consumers worse off overall. Consumers have interests not just in privacy, but also in publicity, access to content, customization, convenience, low prices, and so on. Many of these interests are in tension with privacy, and giving consumers privacy at the cost of other things they prefer is not a good outcome.

The dominant model for producing Internet content—all the interaction, commentary, news, imagery, and entertainment that has the Internet thriving—is advertising support. Many of the most popular services and platforms are "free" because they host advertisements directed at their visitors and users. Part of the reason they can support themselves with advertising is because they have good information about users that allow ads to be appropriately targeted. It is a fact that well-targeted ads are more valuable than less-well-targeted ads.

This is important to note: Most web-based businesses do not "sell" information about their users. In targeted online advertising, the business model is generally to sell advertisers access to people ("eyeballs") based on their demographics. It is not to sell individuals' personal and contact info. Doing the latter would undercut the advertising business model and the profitability of the websites carrying the advertising.

If privacy regulation "blinded" sites and platforms to relevant information about their visitors, the advertising-supported model for Internet content would likely be degraded.

Consumers would be worse off—entombed by an excess of privacy when their preferences would be to have more content and more interaction than regulation allows advertising to support.

If the Federal Trade Commission's recommendations for "notice, choice, access, and security" had been fully implemented in 2000, for example, it is doubtful that Google would have had the same success it has had over the last decade. It might be a decent, struggling search engine today. But, unable to generate the kind of income it does, the quality of search it produces might be lower, and it may not have had the assets to produce and support fascinating and useful products like Gmail, Google Maps, Google Docs, and the literally dozens of author products it provides consumers.[28]

Not having these things at our fingertips is difficult to imagine—it is much easier to assume that the Google juggernaut was fated from the beginning—but the rise of Google and all the access to information it gives us was contingent on a set of circumstances that allowed it to target ads to visitors in a highly customized and—to some—privacy-dubious way.

As a thought experiment, imagine taking away Google, Facebook, Apple's suite of consumer electronics (and the app universe that has sprung up within it), and the interactivity that AT&T facilitates. Consumers would rightly howl at the loss of richness to their lives, newly darkened by privacy. And we would all be worse off as the economy and society were starved of access to information.

All this is just to show that trading on personal information can make consumers better off overall. It is not to say that Google or any other company is the be-all and end-all, or that public policy should do anything to "prefer" any company. In

[28] *See* Wikipedia "List of Google products" page *http://en.wikipedia.org/wiki/List_of_Google_products*.

fact, the other way that privacy regulation might work "too well" is by giving today's leading firms an advantage against future competitors.

A "barrier to entry" is something that prevents competition from entering a market. Barriers to entry often allow incumbents (like the established companies joining me at the witness table today) to charge higher prices and make greater profits than they otherwise would. Common barriers to entry (fair or unfair) include customer loyalty, economies of scale, control of intellectual property, and network effects, to name a few.

Government regulation can act as a barrier to entry in a few different ways. Aside from direct regulation of entry through licensing or grants of monopoly (issues not relevant here), incumbent firms can comply with regulations at a lower cost per sales unit. With a staff of lawyers already in place, the cost per customer of interpreting and applying any regulation are lower for large firms. Whether regulation is merited and tailored or not, small competitors "pay more" to comply with it. Regulation impedes their efforts to challenge established firms.

Established firms can strengthen this dynamic by taking part in crafting legislation and regulation. Their lobbyists, lawyers, and interest-group representatives—the good people gathered at this hearing today—will crowd around and work to protect their clients' interests in whatever comes out of the drafting process, here in Congress and at whatever agency implements any new law. Small, future competitors—unrepresented—will have no say, and new ways of doing business those competitors might have introduced may be foreclosed by regulation congenial to today's winners.

In his paper, *The Durable Internet*,[29] my colleague, Cato adjunct fellow Timothy B. Lee, provides a useful history of how regulatory agencies have historically been turned to protecting the companies they are supposed to regulate. This would occur if the FCC were to regulate Internet service under a "net neutrality" regulation regime. It would occur if a Federal agency were tasked with protecting privacy. It appears to have happened with the Minerals Management Service. The dynamic of "agency capture" is a mainstay of the regulatory studies literature.

Returning to the example of Google and the FTC's proposal for comprehensive regulation a decade ago: Had Congress given the FTC authority to impose broad privacy/fair information practice regulations, companies like Microsoft and Yahoo! may have turned the regulations to their favor. Today, the company the produces that most popular operating system might still be the most powerful player, and we might still be accessing the web through a portal. Consumers would be worse off for it.

For all the benefits today's leading companies provide, there is no reason they should not be subjected to as much competition as our public policy can allow. The spur of competition benefits consumers by lowering prices and driving innovations. Privacy regulation might work "too well" for them, locking in competitive advantages that turn away competition and allow them super-normal profits.

Comparisons between existing companies and future competitors are one thing. But a major defect of most proposals for privacy protection are their bald omission of an entire category of privacy threat: governments.

Privacy for Consumers But Not for Citizens?

Just as people do not have one set of privacy interests for the online world and one for offline, they do not have one set of privacy interests for commerce and another set for government. The privacy protections Americans have as consumers should be made available to them as citizens.

Indeed, given the unique powers of governments—to take life and liberty—Americans should have greater privacy protections from government than they do from private sector entities.

Governments thrive on information about people. Personal information allows governments to serve their citizenry better, to collect taxes, and to enforce laws and regulations. But governments stand in a very different position to personal information than businesses or individuals. Governments have the power to take and use information without permission. And there is little recourse against governments when they use information in ways that are harmful or objectionable.

In the modern welfare state, governments use copious amounts of information to serve their people. A program to provide medical care, for example, requires the government to collect a beneficiary's name, address, telephone number, sex, age, income level, medical condition, medical history, providers' names, and much more.

---

[29] Timothy B. Lee, "The Durable Internet: Preserving Network Neutrality without Regulation," Cato Policy Analysis No. 626 (Nov. 12, 2008) *http://www.cato.org/pub_display.php?pub_id=9775*.

Governments also use personal information to collect taxes. This requires massive collections of information without regard to whether an individual views it as private: name, address, phone number, Social Security number, income, occupation, marital status, investment transactions, home ownership, medical expenses, purchases, foreign assets. The list is very, very long.

A third use government makes of personal information is to investigate crime and enforce laws and regulations. Governments' ability to do these things correlates directly to the amount of information they can collect about where people go, what they do, what they say, to whom they say it, what they own, what they think, and so on. We rely on government to investigate wrongdoing by examining information that is often regarded as private in the hands of the innocent. It is a serious and legitimate concern of civil libertarians that government collects too much information about the innocent in order to reach the guilty. The incentives that governments face all point toward greater collection and use of personal information about citizens. This predisposes them to violate privacy.

Yet "consumer privacy" bills planned and introduced in the current Congress do nothing to protect Americans' privacy from government. The leading proposals in the House—Rep. Boucher's (D–VA) draft legislation and H.R. 5777, the "BEST PRACTICES Act," introduced by Rep. Rush (D–IL)—simply exclude the Federal Government from their provisions.

In fairness, there may be jurisdictional reasons for these exemptions, but the hypocrisy would be a little too rank if the Federal Government were to impose privacy regulations on the private sector while its own profligacy with citizens' information continues.

If there is to be privacy legislation, the U.S. Congress should demonstrate the commitment of the Federal Government to getting its own privacy house in order. The Federal Government should practice what it preaches about privacy.

Conclusion

Privacy is a complicated human interest, of that there should be no doubt. In this long written testimony I have only begun to scratch the surface of the issues.

People use the word privacy to refer to many different human interests. The strongest sense of the word refers to control of personal information, which exists when people have legal power to control information and when they exercise that control consistent with their interests and values.

Direct privacy legislation or regulation is unlikely to improve on the status quo. Over decades, a batch of policies referred to as "fair information practices" have failed to take hold because of their complexity and internal inconsistencies. In the cases when they have been adopted, such as in the Privacy Act of 1974, privacy has not blossomed.

Even modest regulation like mandated privacy notices have not produced privacy in any meaningful sense. Consumers generally do not read privacy policies and they either do not consider privacy much of the time or value other things more than privacy when they interact online.

The online medium will take other forms with changing times, and regulations aimed at an Internet dominated by the World Wide Web will not work with future uses of the Internet, as we are beginning to see in handheld devices. Privacy regulations that work "too well" may make consumers worse off overall, not only by limiting their access to content, but by giving super-normal profits to today's leading Internet companies and by discouraging consumer-friendly innovations.

It is an error to think that there are discrete "online" and "offline" experiences. Consumers do not have separate privacy interests for one and the other. Likewise, people do not have privacy interests in their roles as consumers, and a separate set of interests as citizens. If the Federal Government is going to work on privacy protection, the Federal Government should start by getting its own privacy house in order.

APPENDIX I

Privacy Advocates Who Don't Understand Privacy

In 2006 an engineer working on an experimental WiFi project for Google wrote a piece of code that sampled publicly broadcast data—the information that unencrypted WiFi routers make available by radio to any receiver within range. A year later, this code was included when Google's mobile team started a project to collect basic WiFi network data using Google's Street View cars.

When Google discovered this issue, they stopped running their Street View cars and segregated the data on their network, which they then disconnected to make

it inaccessible.[30] Google announced the error to the public and have since been working with European data authorities to try to get rid of it. The European authorities are making them keep it pending their investigations.

Now a U.S. advocacy group, tripping over itself to make this a Federal issue, has done more to invade privacy than Google did.

WiFi nodes are like little radio stations. When they are unencrypted, the data they send out can be interpreted fairly easily by whoever receives the radio signals.

Radio signals can travel long distances, and they pass through or around walls and vehicles, people, shrubs and trees. Broadcasting data by radio at the typical signal-strength for a WiFi set-up creates a good chance that it is going to travel outside of one's house or office and beyond one's property line into the street.

For this reason, people often prevent others accessing the information on Wifi networks by encrypting them. That is, they scramble the data so that it is gibberish to anyone who picks it up. (Or at least it takes an enormous amount of computing power to unscramble the signal.) Most people encrypt their WiFi networks these days, which is a good security practice, though it denies their neighbors the courtesy of using a handy nearby Internet connection if they need to.

Even on an unencrypted WiFi network, much sensitive content will be encrypted. Transactions with banks or payments on commerce sites will typically be encrypted by the web browser and server on the other end (the "s" in "https:" indicates this is happening), so their communications are indecipherable wherever they travel.

Given all this, it's hard to characterize data sent out by radio, in the clear, as "private." The people operating these unsecure WiFi nodes may have *wanted* their communications to be private. They may have thought their communications were private. But they were sending out their communications in the clear, by radio—again, like a little radio station broadcasting to anyone in range.

Picking up the data it did using its Street View cars, Google captured whatever it did during the few seconds that the car was in range of the unencrypted WiFi node. The flashes of data would be quite similar to driving past a row of apartments and seeing snippets of life inside whichever apartments had not fully drawn their curtains. Often, there is nothing happening at all. Once in a while, there may be a flicker of something interesting, but it is not tied to any particular identity.

Google never used this useless data. Not a single fact about a single identifiable WiFi user has been revealed. No personal information—much less private information—got any meaningful exposure.

But a U.S. advocacy group seeking to make a Federal case of this story tripped over its privacy shoelaces in doing so. Apparently, researchers for this self-described consumer organization looked up the home addresses of Members of Congress. They went to the homes of these representatives, and they "sniffed" to see if there were WiFi networks in operation there. Then they publicized what they found, naming Members of Congress who operate unencrypted WiFi nodes.

If you care about privacy, this behavior is worse than what Google did. In its gross effort to rain attention on Google's misdeed, this group collected information on identifiable individuals—these Members of Congress—and put that information in a press release. That is more "stalkerish" and more exposing of personal information than driving past in an automobile picking up with indifference whatever radio signals are accessible from the street.

The behavior of this group is not a privacy outrage. Politicians volunteer to be objects of this kind of intrusion when they decide that they are qualified to run for Federal elective office. It simply illustrates how difficult the "privacy" issue is, when a group pulling off a stunt to draw attention to privacy concerns does more harm to privacy than the "wrongdoer" they are trying to highlight.

APPENDIX II

Facebook's "News Feed": Consumers Privacy Interests are Unpredictable and Changing

In September 2006, Facebook—the rapidly growing "social networking" site—added a feature that it called "News Feed" to the home pages of users. News Feed would update each user regularly on their home pages about the activities of their friends, using information that each friend had posted on the site.[31] "News Feed"

---

[30] *See* "WiFi Data Collection: An Update," the Official Google Blog (May 14, 2010) *http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html*.

[31] *See* "Facebook Gets a Facelift," The Facebook Blog (Sept. 5, 2006) *http://blog.facebook.com/blog.php?post=2207967130*.

was met with privacy outrage.[32] In the view of many Facebook users, the site was giving too much exposure to information about them.

But Facebook pushed back. In a post on the Facebook blog titled, "Calm down. Breathe. We hear you,"[33] CEO Mark Zuckerberg wrote:

> This is information people used to dig for on a daily basis, nicely reorganized and summarized so people can learn about the people they care about. You don't miss the photo album about your friend's trip to Nepal. Maybe if your friends are all going to a party, you want to know so you can go too. Facebook is about real connections to actual friends, so the stories coming in are of interest to the people receiving them, since they are significant to the person creating them.

Though Facebook did make some changes, users ultimately found that News Feed added value to their experience of the site. Today, News Feed is an integral part of Facebook, and many users would probably object vociferously if it were taken away.

This is not to say that Facebook is always right or that it is always going to be right. It illustrates how consumers' privacy interests are unsettled and subject to change. Their self-reported interests in privacy may change—and may change rapidly.

The Facebook "News Feed" example is one where consumers looked at real tradeoffs between privacy and interaction/entertainment. After balking, they ultimately chose more of the latter.

Consider how well consumers might do with privacy when they are not facing real tradeoffs. Consumer polling on privacy generally uses abstract questions to discover consumers' stated privacy preferences. There is little policymaking value in polling data.[34] Determining consumers' true interests in privacy and other values is difficult and complex, but it is taking place every day in the rigorous conditions of the marketplace, where market share and profits are determined by companies' ability to serve consumers in the best ways they can devise.

Some economic studies have suggested how much people value privacy.[35] The goal of privacy advocacy should not be to force unwanted privacy protections on a public that does not want them, but to convince consumers to value privacy more.

The CHAIRMAN. Thank you, sir.

Mr. Dorothy Attwood, Senior Vice President of Public Policy, and Chief Privacy Officer, AT&T.

STATEMENT OF DOROTHY ATTWOOD, SENIOR VICE PRESIDENT, PUBLIC POLICY AND CHIEF PRIVACY OFFICER, AT&T, INC.

Ms. ATTWOOD. Thank you, Chairman Rockefeller and Ranking Member Hutchison, for providing AT&T, today, with the opportunity to participate in this hearing.

For the 2 billion of us who access the Internet, the possibilities are boundless. The Internet is a venue for almost every type of human interaction. From love to money, we search for it on the Web. Yet, we only have glimpsed the possibilities. Digital signals sent from the rubble in Haiti enabled relief workers to locate earthquake survivors. Electric grids can be organized and managed efficiently, thanks to the instant interexchange of information over broadband networks. Businesses can cut costs by storing data in the cloud.

But, these advantages are not guaranteed. At its heart, the Internet runs on information shared willingly among its users. The

---

[32] *See* Michael Arrington, "Facebook Users Revolt, Facebook Replies" TechCrunch (Sept. 6, 2006) *http://techcrunch.com/2006/09/06/facebook-users-revolt-facebook-replies/*.

[33] "Calm down. Breathe. We hear you," The Facebook Blog (Sept. 5, 2006) *http://blog.facebook.com/blog.php?post=2208197130*.

[34] Jim Harper and Solveig Singleton, "With a Grain of Salt: What Consumer Privacy Surveys Don't Tell Us" (June, 2001) *http://cei.org/PDFs/with_a_grain_of_salt.pdf*.

[35] Alessandro Acquisti at Carnegie Mellon University has made a specialty of studying how consumers value privacy. *http://www.heinz.cmu.edu/acquisti/*.

continued growth of the Internet, as well as its positive social and economic benefits, are dependent upon earning and maintaining the trust, of Internet users, that their information is being shared in the way they intend.

When I appeared before this committee 2 years ago, I articulated the four pillars of AT&T's approach to our customers' privacy: transparency, customer control, privacy protection, and consumer value. We urged then, and we continue to believe, that these principles can be the foundation of a privacy regime applicable to all entities in the online ecosystem. Indeed, we're now even more convinced that consumers have a consistent set of expectations about their privacy that should be met by a consistent standard used throughout the Internet.

Last summer, AT&T, through an open and inclusive rollout process that incorporated a 45-day preview period and comments from our customers, adopted a new plain-language privacy policy that applies to all AT&T services. In consolidating 17 policies into one, we recognized that, when it came to privacy, our customers' expectations are the same, regardless of the nature, let alone the legacy regulatory classification, of the services they purchase. They want their privacy to be respected and regard the information they share as theirs to govern.

AT&T has also emphasized "privacy by design" as a means of increasing transparency and the availability of privacy-enhancing technologies by ensuring these features are built in at the outset, rather than added on as an afterthought. For example, earlier this year we added an "Advertising Choices" link onto our *yp.com* website that explains our use of what customers search for on *yp.com* to target ads to users elsewhere on the Internet, tells them how to opt-out of their use of that information, and how to locate the interest category or profile manager that we developed.

We also launched an advertising-supported social-networking recommender site called "*buzz.com.*" Users cannot join this information-sharing site without first establishing their privacy preferences. We provide additional notice about information-sharing on the site through a separate link, and we call it what it is, "information sharing," not "privacy."

Other industry groups have, likewise, made important progress in standardizing the users' experience so they can better understand the use of their online information for targeted advertising. The IAB has unified the presentation of the NAI opt-out tool and adopted an icon that will be used throughout the industry. AT&T is building on this momentum by working with better advertising to trial inclusion of the icon in certain of its ads, and with TRUSTe on behavioral advertising pilot seal program.

We believe the industry should press even further, however, and develop a trust framework that enables the interoperability of permissions. With this framework, entities throughout the Internet ecosystem could cooperate in a back-office way to honor the information-sharing preferences of the customer.

Such an approach can be likened to banking, where consumers initiating fund transfers are not involved in the details of when and how the automated clearinghouse handles the actual money

transfers, but they have every confidence that their money goes where they intend.

As detailed in my written testimony, groundbreaking work on such a trust-based ecosystem is already underway. It's easy to misinterpret the ease with which personal information is shared to mean that those sharing information are unconcerned about privacy. We don't think that's accurate. Privacy on the Internet is not the inverse of security, but, instead, it's about the creation and maintenance of an online identity. And consumers want control over the creation and sharing of that identity. We've seen, time and again, that users choosing to share their information is entirely different from companies choosing to share information about their users.

It's beyond question that consumer information is the bedrock of online advertising, which, in turn, fuels a great deal of Internet investment and innovation. At the same time, we need to address the fundamental issue of how to preserve customer confidence and trust in the Internet. Working together, government and industry must take the bold step of moving beyond a balkanized system of notice and consent to a truly consumer-centric framework for information-sharing that will grow trust and confidence and keep the economic engine of the Internet running through successive decades of innovation.

Thank you.

[The prepared statement of Ms. Attwood follows:]

PREPARED STATEMENT OF DOROTHY ATTWOOD, SENIOR VICE PRESIDENT, PUBLIC POLICY AND CHIEF PRIVACY OFFICER, AT&T INC.

Thank you, Chairman Rockefeller and Ranking Member Hutchison, for providing AT&T with another opportunity to participate in a thoughtful examination of how consumer information is shared in the online world and what role those doing the sharing have in creating a comprehensive, consumer-centric approach to online privacy.

Background

For those of us who access the Internet—perhaps 2 billion people worldwide—the online possibilities are boundless. It is a venue for almost every type of human interaction or transaction. We can connect with old friends and meet new ones, purchase every imaginable good or service, find answers to almost every question, do business with our bank, exchange health information with our doctor, access libraries, get services from the government, communicate with political leaders, organize social events, mobilize a community, or facilitate disaster recovery. From love to money, we search for it on the Web.

Yet, for all that we already do on the Internet, we have only glimpsed the possibilities. Digital signals from the earthquake rubble of Haiti enabled relief workers to locate survivors, direct food and medicine delivery, and map transportation options to expedite emergency efforts. GPS data from wireless networks can be assembled to observe the flow of people, services, and cars so that urban planners can build more livable cities. Electric grids and other infrastructure can be organized and managed for efficiency thanks to the instant exchange of information over broadband networks. Businesses can cut costs by storing data in the cloud or use Web data to create tailored services for their customers.

But these advances are not guaranteed. At its heart, beyond the computing power, software and backbone networks, the Internet runs on information shared willingly among its users. This sharing requires confidence and trust that the personal information we provide is safe from abuse and will be used in ways that we approve. Even in a digital world, most people continue to value their privacy—although they may approach their privacy differently from the way they did before the Internet entered our lives. Thus, the continued growth of the Internet, and the positive social and economic benefits of that growth, are dependent upon earning, maintaining and

preserving the confidence and trust of Internet users worldwide that their information is being shared in the way they intend.

Online Privacy: Where We Started and What We've Learned

Two years ago when I appeared before this committee, I articulated the four pillars of AT&T's approach to our customers' privacy: transparency, consumer control, privacy protection and consumer value—all designed to create and preserve our customers' trust. We urged then, and we continue to believe, that these principles can be the foundation of a consistent regime applicable to all entities in the online ecosystem that inspires trust in users worldwide. At the same time we have learned through practical experience that, as good as the various individual privacy efforts and consensus best practices are, more concerted activity is needed across the entire Internet ecosystem. Consumers have a consistent set of expectations about their privacy wherever they go online, regardless of which portals they enter and the number of places they visit. In light of this, there ought to be consistent standards to meet those expectations throughout the Internet ecosystem. We are even more convinced today that the changing Internet marketplace requires a privacy regime that moves beyond the current patchwork of ad hoc practices for providing notice and obtaining consent to an interoperable framework—one in which a customer's consents and preferences are honored throughout the Internet ecosystem.

Transparency and Customer Control

Since I last testified before this Committee, AT&T and others in the industry have developed a variety of innovative solutions that are the essential steppingstones to the next phase in the evolution of online privacy practices. For example, last summer AT&T, through an open and inclusive roll-out process that specifically incorporated a 45-day preview period and comments from our customers, adopted a new, simplified, plain language privacy policy that applies to all AT&T services. Companies everywhere have come to the realization that privacy policies need to be readable and understandable, and we're especially proud of the way we have implemented transparency and control at the very outset of our customer relationship.

In consolidating 17 separate written company privacy policies into a single, unified, easy-to-understand AT&T privacy policy, we recognized that there was no reason for treating AT&T Mobility customer relationships different from AT&T U-Verse customer relationships or AT&T Long Distance customer relationships—and on down the line. Our customer's privacy expectations are the same regardless of the nature, let alone legacy regulatory classifications, of the services they purchase from us. Our experience as the leading communications company in America with a diverse wireless, wireline, and video portfolio, combined with our experience as a major online advertiser, a website publisher, and Internet service provider, helped us to appreciate that customers not only want a clear understanding of how they can control the sharing of their personal information, but they want their expectations honored consistently regardless of what they do or where they go online. Bottom line, our Internet users want their privacy to be respected, and regard the information they share as theirs to govern.

AT&T's Innovation Through Privacy By Design

AT&T has also emphasized bringing privacy-enhancing technologies to consumers through the roll out of new products, including the online advertising space, where we have actively improved our transparency as an advertiser and publisher. We apply these principles at the start of product development and strategy by embedding transparency and control features into the product itself, not as an add-on or afterthought. We have added an "advertising choices" link on our "YP.com" yellow pages website that explains how and where we use what consumers search for on *YP.com* to target ads to users elsewhere on the Internet. This link also explains to users how to opt-out as well as how to discover the "interest" category—or profile manager—that we have developed, and permits users to modify that profile. Essentially, we offer customers the ability to view and edit the interest categories that we have associated with them and a simple process for them to choose not to be targeted in this way.

We have also launched an advertisement-supported social networking "recommender" site that we call "Buzz.com." *Buzz.com* combines aspects of social networking with local search, so that users can search local listings for a restaurant or a doctor and get recommendations from people that users know as well as from other *Buzz.com* users in general. Because the site is based upon information sharing, users cannot join the site without first establishing their privacy preferences. We provide notice to our customers beyond the official notice in the general privacy policy through a separate link entitled "Things you should know about how your information is shared on buzz.com." Indeed, we call it what is—information sharing

not privacy—and go the extra mile to explain the details of the information sharing that takes place. Specifically, we give our customers a number of choices that permit them to control the scope and extent of that information sharing during the initial registration process. We explain the different levels of information sharing in plain language and make clear that "anonymous" postings may not always stay that way, so that customers are not surprised down the road.

We believe these new capabilities not only represent an example of an industry best practice but also demonstrate that technological innovations can and do occur when firms embrace privacy by design—that is, when they design their customer facing offerings in a way that provides both transparency and meaningful tools to control whether and how their information is shared. For example, providers of location-based services have demonstrated that functional integration of customer permissions can spur the acceptance of these new services. Indeed, location-based services continue to grow and incorporate consumer permission processes into the sign up and use of the service itself. Importantly, CTIA has established best practices and guidelines for entities that provide location-based services, including mobile operators, device manufacturers and applications developers that encourage industry-wide adoption of robust permission-based approaches as well as further innovations in privacy enhancing technologies.

Ecosystem Evolution of Online Privacy

Other industry groups have likewise come together to make important progress in standardizing, clarifying and simplifying the user's understanding and control of how their online experience is used for targeted advertising. For example, the Internet Advertising Bureau has unified the presentation of the NAI opt-out tool, and adopted an icon that will be used throughout the industry to increase transparency. AT&T is helping to build on this momentum by working with Better Advertising to trial inclusion of the icon in certain of its ads, and by participating with TRUSTe on its behavioral advertising pilot seal program, which is designed to give customers confidence that their privacy trust is well placed. All of these steps represent important progress toward an ecosystem-wide approach based on customer engagement and the ultimate goal of giving customers the tools necessary to manage their online identity in one place, at one time, so that their preferences are respected wherever they travel on the Internet.

Building on this progress, we believe the industry, which has innovation in its very DNA, should press even further and develop a trust framework that enables the "interoperability of permissions." With this framework, entities throughout the Internet ecosystem could cooperate in a "back-office" way to honor the information sharing preferences of the customer. Such an approach can be likened to the existing process in banking, where consumers initiating fund transactions are not involved in the details of when and how the automated clearing houses handle the actual money transfers, but have every confidence that their money goes when and where they intend.

Ground-breaking work on such a trust based ecosystem is already underway. For example, a draft White House report made public in June maps out a framework for "trusted identities in cyberspace" and suggests a "user-centric model" based around individual preferences. Private entities are working on user-centric identity management tools ("IDM tools") that give consumers the opportunity to decide how much of their identity to reveal, when and to whom. The two most prominent IDM tools, "OpenID" and "Information Cards" put the user in control of identity-based interactions and potentially provide a uniform user-driven approach to data collection and use. In addition, private companies are developing other technologies—browser controls, widgets and downloads—that will enable users to set and manage their privacy preferences. Firefox, for example, offers consumers a browser add-on that protects and automatically updates opt-out settings, including flash cookie controls. Tracker Watcher, another browser add-on, offers users a way of identifying companies that track consumer online behaviors.

These tools have the potential to improve users' online experience and enhance privacy. For example, IDM tools have the potential to be used to establish privacy preferences, minimize the disclosure of personal, identifying information, enhance user choice about the nature and amount of data to be shared, and expand users' say regarding the timing and manner of updating and withdrawing data. Such tools also could provide websites with a secure, standardized means of authenticating users.

Conclusion

It is easy to misinterpret the ease with which personal information is shared to mean that those sharing information are unconcerned about privacy. We don't think

that is accurate. Privacy is a more multi-dimensional idea on the Internet. It is not the inverse of security, but instead is about the creation and maintenance of an online identity—and consumers want control over how they present themselves online, and with whom and where they share information. We have seen time and again that users choosing to share their information is entirely different from companies choosing to share information about their users.

Policy makers and industry should work together to promote an Internet that promotes permission-based, user-driven sharing of information in a safe and secure environment. It is beyond question that consumer information is the bedrock of online advertising, and that online advertising fuels a great deal of the investment and innovation across a wide range of Internet activities, providing the revenue that enables consumers to continue to enjoy a myriad of free and discounted services. Indeed, website publishers continue to make most of their money from advertising, which in turn funds the breadth and diversity of today's Internet content and information that is, in most cases, made available to consumers for free. At the same time, the lack of consumer trust in the Internet threatens to undermine the American economy. So we are back to the fundamental bedrock issue of how to preserve consumer confidence and trust in the Internet. Working together, government and industry must take the bold step of moving beyond a balkanized system of notice and consent regimes that seem more about the entities that are collecting consumer information than the rights of consumers in controlling that information. By doing so, we can maintain the consumer trust and confidence that will keep the economic engine of the Internet running through successive decades of innovation.

The CHAIRMAN. Thank you very much.

And finally, Professor Joseph Turow, who's—at the Annenberg School for Communication.

Mr. TUROW. Thank you.

The CHAIRMAN. We welcome you back.

STATEMENT OF JOSEPH TUROW, PH.D.,
ROBERT LEWIS SHAYON PROFESSOR OF COMMUNICATION,
THE ANNENBERG SCHOOL FOR COMMUNICATION,
UNIVERSITY OF PENNSYLVANIA

Mr. TUROW. Thank you. Thank you, Chairman Rockefeller and the other committee members, for providing me the——

The CHAIRMAN. Turn your mic on.

Mr. TUROW.—for providing—oh, sorry—for providing me the opportunity to contribute to this discussion. I'd like——

The CHAIRMAN. You know what——

Mr. TUROW.—to highlight——

The CHAIRMAN.—you're still a little hard to hear.

Mr. TUROW. Sorry.

The CHAIRMAN. That's because you're off the end of the table.

Mr. TUROW. Yes. Well—OK. I would like to highlight——

The CHAIRMAN. There we go.

Mr. TUROW.—four points of my written testimony.

The first is, we have a whole new world here. And, Chairman Rockefeller, your beginning statement, I think, really exemplified what's going on. It used to be that media firms sold segments of large populations through media outlets. Today, a detailed level of knowledge about people and their behaviors are being used in ways that were unheard of just a few years ago. It's now increasingly common to buy the right to deliver an ad to a person with specific characteristics at the precise moment that that person loads a web page. In fact, through cookie-matching activities, an advertiser can actually buy the right to reach someone on an exchange whom the advertiser knows—from previous contacts, and is now tracking around the Web.

Point two: Industry claims of anonymity undermine the traditional meaning of the word "anonymity." If a company can follow your behavior in the digital environment, and that includes the mobile phone and, potentially, your television set, its claim that you're anonymous is meaningless. Because we live so much of our lives in the digital arena, if they know I'm Joseph Turow or X53ZV, it doesn't matter, because they're following me and presenting me with certain views of the world.

And more and more, we have a cavalcade of companies that are contributing. Not just the companies, the big firms that are here; companies that—just off the top of my head, eXelate, Rapleaf, BlueKai, Experian, Medicx Media Solutions—that contribute data they hold that can create quite a detailed picture of us, but we don't know it, and we don't give our permission about it, and sometimes may even harm our reputation. So, essentially, reputations are being created here.

Point three: People care a lot about data collection, but don't know what's going on. National surveys I've conducted at the Annenberg School since 1999 consistently show that, in large proportions, American adults do not understand how the new data-based marketing process that take place behind their screens work. And we found that over and over again. Privacy policies don't help.

And I hate to be a negativist, but I'm very concerned that the box we've been talking about could bring the kind of problems that we've heard about regarding privacy policies.

It's clear to me, for example, that newer tools, sometimes called "dashboards," are counterproductive in some cases. These are tools, as we've heard, that firms, such as Google, provide for consumers to learn what the companies know about them. The reason dashboards are counterproductive, so far, is that they provide visitors with the incorrect impression that they fully reveal the information advertisers use to address them on those sites.

I'd like to suggest to the Senators that they ask the Google representative whether the data available about us in the Google Display Network are really limited by what shows up about us on Google's Dashboard.

The Annenberg study I mentioned also show consistently that Americans know their activities are being followed online, and are deeply uncomfortable and concerned about it.

A recent national survey I conducted with researchers at UC Berkeley Law School showed, emphatically, that Americans don't want a situation where content is tailored for them based on the firm's use of their data without their knowing it. Unfortunately, the situation they don't want is getting worse.

And so, I would suggest that the emerging digital world raises serious consumer protection issues. When companies track people without their knowledge, sell their data without their knowledge or permission, and then decide whether they are, in the words of the industry, "targets" or "waste," we have a social problem. If it's allowed to fester, and when Americans begin to realize how it pits them against others in the ads they get, the discounts they receive, the TV Guide suggestions they're going to get, and the news stories they confront, and even the offers that they get relating to other parts of the world, we're in a situation—for example, in the super-

market—they'll get even more disconcerted and angry than they are now.

So, we have to move from the current marketing regime that uses information with abandon, where people's data are being sliced and diced to create reputations for them that they don't know about and might not agree with, to a regime that acts toward information with respect. That is where marketers recognize that people own their data, have rights to know where all their data are collected and used, and should not have to worry, when they travel through the media world, that their actions and backgrounds will cause them unwarranted social discrimination regarding what they later see and hear.

So, I suggest that, to help the public, Congress should recognize that certain aspects of this new world raise serious consumer protection issues, and act with that in mind. One path might be to limit the extensiveness of data, or clusters of data, that a digital advertiser could keep about an individual or household.

Some industry organizations resist such suggestions, depicting scenarios of Internet doom if Congress moves forward with privacy regulations regarding digital platforms. But, in the face of Americans' widespread concerns about the exploitation of their data, a level regulatory playing field, in the interests of privacy, will actually have the opposite effect. It will increase public trust in online actors and set the stage for new forms of commercial competition from which industries and citizens will benefit.

And I thank the Committee for inviting me. Look forward to your questions.

[The prepared statement of Mr. Turow follows:]

PREPARED STATEMENT OF JOSEPH TUROW, PH.D., ROBERT LEWIS SHAYON PROFESSOR OF COMMUNICATION, THE ANNENBERG SCHOOL FOR COMMUNICATION, UNIVERSITY OF PENNSYLVANIA

I thank Chairman Rockefeller, Ranking Member Kay Bailey Hutchinson and the other committee members for providing me the opportunity to contribute to this discussion. As a professor at the University of Pennsylvania's Annenberg School for Communication, I have been conducting research and writing about new media and marketing for over two decades. In addition to many articles, I have written two books directly on the topic and co-edited two others. I am currently finishing a book about digital marketing for Yale University Press.

I come to this hearing as a media sociologist who cares deeply about Americans' ability to trust the companies we deal with, to get along with each other, and to believe that the government will protect us when we cannot protect ourselves. Each of these values is being threatened by the data policies of companies throughout our media system. Let me explain in four points.

Point 1: We have a whole new world here. Prior to the digital revolution, marketers used media such as newspapers, magazines, radio, outdoor boards, and television to reach out to segments of the population. Marketers typically learned about these audience segments by using data from survey companies that polled representative portions of the population via a variety of methods, including panel research. Less commonly, they sent questionnaires to people they knew were readers or listeners.[1]

The emerging new world is dramatically different.[2] Instead of large populations and population segments as audiences, advertisers now expect media firms to deliver to them very particular types of individuals—and increasingly particular individuals—with a detailed level of knowledge about them and their behaviors that

[1] See, for example, Joseph Turow, *Breaking Up America: Advertisers and the New Media World* (Chicago: University of Chicago Press, 1997), pp. 18–37.

[2] For a historical overview, see Joseph Turow, *Niche Envy: Marketing Discrimination in the Digital Age* (Cambridge: MIT Press, 2006), pp. 44–98.

was unheard of even a few years ago. Special online advertising exchanges, owned by Google, Yahoo!, Microsoft, Interpublic and other major players, allow for the auction of individuals with particular characteristics often in real time. That is, it is now possible to buy the right to deliver an ad to a person with specific characteristics at the precise moment that the person loads a web page. In fact, through cookie matching activities, an advertiser can actually buy the right to reach someone on an exchange whom the advertiser knows from previous contacts and is now tracking around the web.

Point 2: Industry claims of anonymity undermine the traditional meaning of the word. With the activities just described has come a new vocabulary that reflects potentially grave social divisions and privacy issues. Marketers talk about people as *targets* and *waste*. Increasingly, they offer individuals different products and discounts based on ideas marketers have gleaned about them without their knowledge. These social differentiations are spreading from advertising to information, entertainment and news, as media firms try hard to please their sponsors. Marketers also use words like *anonymous* and *personal* in ways that have lost their traditional meaning. If a company can follow your behavior in the digital environment—and that potentially includes the mobile phone and your television set—its claim that you are anonymous is meaningless. That is particularly true when firms intermittently add offline information to the online data and then simply strip the name and address to make it "anonymous."

The business arrangements that use this new language are transforming the advertising and media landscapes. Companies track people on websites and across websites with the aim of learning what they do, what they care about, and whom they talk to. Firms that exchange the information often do keep the individuals' names and postal addresses anonymous, but not before they add specific demographic data and lifestyle information. Here are just three examples:

- eXelate is a leading targeting exchange with the motto "data anywhere. audience everywhere."[3] It determines a consumer's age, sex, ethnicity, marital status, and profession by partnering with websites to scour website registration data. It also tracks consumer activities online to note, for example, which consumers are in the market to buy a car or are fitness buffs, based on their Internet searches and the sites they frequent. It sells these packages of information about individuals as cookie data so advertisers can target them.[4]
- Rapleaf is a firm that says it helps marketers "customize your customers' experience."[5] To do that, it gleans data from individual users of blogs, Internet forums, and social networks. It uses ad exchanges to sell the ability to reach those individual cookies. The company says it has "data on 900+ million records, 400+ million consumers, [and] 52+ billion friend connections."[6]

A company called Medicx Media Solutions links "HIPAA certified medical and pharmacy insurance claims data"[7] for tens of millions of Americans to information about them from information suppliers such as Experian as well as from health surveys people fill out. Even though Medicx cannot tie the data to particular individuals, it does retain an ability to connect the medical, pharmacy, and survey findings to ZIP+4 postal clusters of 3–8 homes where, it says, "the incidence of any specific disease is three (3) to twenty (20) times what it is in the general population."[8] To reach these patients for advertisers, Medicx licenses millions of cookies with ZIP+4 data and then serves its clients' display ads to cookied individuals in the targeted ZIP+4 areas. The people receiving the ads about specific medical concerns would have no clue how they got them.

Point 3: People care a lot about data collection but don't know what is going on: What I have just described is the tip of an iceberg of what goes on behind Americans' screens. National surveys that I have conducted since 1999 consistently show that in large proportions American adults know their activities are being followed

---

[3] *http://exelate.com/new/index.html* , accessed July 23, 2010.
[4] See the exelate website: *http://exelate.com/new/index.html* , accessed July 23, 2010.
[5] *http://www.rapleaf.com/*, accessed July 23, 2010.
[6] Rapleaf, Webinar on "How to Market to Your Influencers," *http://www.slideshare.net/Rapleaf/how-to-market-to-your-influencers-3530390* (slide 3), accessed July 23, 2010.
[7] [No author], "Mindset Marketing Solutions Debuts Zip+4 Geomedical Targeting With Launch of geoMEDICX," PRWeb, November 7, 2008, *http://www.prweb.com/releases/2008/11/prweb1576174.htm*.
[8] [No author], "Mindset Marketing Solutions Debuts Zip+4 Geomedical Targeting With Launmch of geoMEDICX," PRWeb, November 7, 2008, *http://www.prweb.com/releases/2008/11/prweb1576174.htm*.

online and are deeply uncomfortable and concerned about it.[9] It is also quite clear from our surveys and other research that Americans do not understand how the processes that surround them work. Few people read privacy policies, and they are in any event uniformly turgid and ambiguous. Some firms provide cookie deletions as a solution to targeting (though not tracking), but marketers and media firms are increasingly finding ways to get around the deletion of cookies. In addition tools sometimes called dashboards that firms such as Google provide for consumers to learn what the companies know about them are counterproductive. That is because they provide visitors with the incorrect impression that the tools fully reveal the information advertisers can use to address them on those sites. I'd like to suggest to the senators that they ask the Google representative whether the data available about us in the Google Display Network are really limited by what shows up about us on Google's dashboard.

Point 4: The emerging digital world raises serious consumer protection issues. There are many great things about the new media environment. But when companies track people without their knowledge, sell their data without their knowledge or permission, and then decide whether they are, in the words of the industry, targets or waste, we have a social problem. A recent national survey I co-conducted showed emphatically that Americans don't want this type of situation.[10] If it's allowed to fester, and when they begin to realize how it pits them against others in the ads they get, the discounts they receive, the TV-guide suggestions and news stories they confront, and even the offers they receive in the supermarket, they will get even more disconcerted and angry than they are now. They will further distrust the companies that have put them in this situation, and they will be incensed at the government that has not helped to prevent it. A comparison to the financial industry is apt. Here was an industry engaged in a whole spectrum of arcane practices not transparent to consumers or regulators that had serious negative impact on our lives. It would be deeply unfortunate if the advertising system followed the same trajectory.

We must move from the current marketing regime that uses information with abandon—where people's data are being sliced and diced to create reputations for them that they don't know about and might not agree with—to a regime that acts toward information with respect. That is where marketers recognize that people own their data, have rights to know where all their data are collected and used, and should not have to worry when they travel through the media world that their actions and backgrounds will cause them unwanted social discrimination regarding what they later see and hear.

Until recently, I believed that educating publics about data collection and giving them options would be sufficient to deal with privacy issues related to advertising. I have come to realize, though, that Americans don't have and will not acquire the complex knowledge needed to understand the increasing challenges of this marketplace. Opt-out and opt-in privacy regimes, while necessary, are far from sufficient. The reason is that people will often have neither the time nor ability to make proper cost-benefit evaluations of how sites and marketers use their data under various opt-in or opt-out choices.

To help the public, Congress should recognize that certain aspects of this new world raise serious consumer protection issues and act with that in mind. One path is to limit the extensiveness of data or clusters of data that a digital advertiser can keep about an individual or household. Some industry organizations resist such suggestions, depicting scenarios of Internet doom if Congress moves forward with pri-

---

[9] See, for example, "The Internet and the Family: The View from Parents, the View from the Press." A Report from the Annenberg Public Policy Center of the University of Pennsylvania under the direction of Joseph Turow, May 1999, 42 pp; Joseph Turow and Lilach Nir, "The Internet and the Family 2000: The View From Parents, the View from Kids." A Report from the Annenberg Public Policy Center of the University of Pennsylvania, 35 pp; "Americans and Online Privacy: The System is Broken." Report of the Annenberg Public Policy Center, June 2003; Joseph Turow, "Open to Exploitation: American Shoppers Online and Offline," Report of the Annenberg Public Policy Center, June 2005. These are available on the Annenberg Public Website: *http://www.annenbergpublicpolicycenter.org/AreaDetails.aspx?myId=2*. See also Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy, "Americans Reject Tailored Advertising and Three Activities That Enable It," Annenberg School for Communication (U of Pennsylvania) and Berkeley School of Law (U California, Berkeley), November 2009 *http://papers.ssrn.com/sol3/papers.cfm?abstract__id=1478214* ; and Chris Jay Hoofnagle, Jennifer King, Su Li, and Joseph Turow (listed in alphabetical order), "How Different are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policies?" April 16, 2010. *http://papers.ssrn.com/sol3/papers.cfm?abstract__id=1589864*.

[10] Americans Reject Tailored Advertising and Three Activities That Enable It," Annenberg School for Communication (U of Pennsylvania) and Berkeley School of Law (U California, Berkeley), November 2009. *http://papers.ssrn.com/sol3/papers.cfm?abstract__id=1478214*.

vacy regulations regarding digital platforms. But in the face of Americans' widespread concern about the exploitation of their data, a level regulatory playing field in the interest of privacy will actually have the opposite impact. It will increase public trust in online actors and set the stage for new forms of commercial competition from which industries and citizens will benefit.

I want to thank the Committee for inviting me today.

The CHAIRMAN. Thank you for that.

I'm going to start with Senator Kerry, who is the Chairman of the Subcommittee on Telecommunications, which is really over all of this.

Senator Kerry.

STATEMENT OF HON. JOHN F. KERRY,
U.S. SENATOR FROM MASSACHUSETTS

Senator KERRY. Mr. Chairman, thank you. And I appreciate your having this hearing, a very, very important topic.

And I'm sorry that I wasn't able to be here for the first panel, as we went over to vote and, unfortunately, wound up—the vote slid backward. So, here we are.

But, I appreciate all of the members of this panel coming forward.

Professor Turow, I appreciate your comments, just now.

I would say—I think it's fair to say that right now there is a lot of confusion and a lot of anxiety among the public at large about what power they have over the collection of information—and over their lives, in the end—and how it all is managed. And it's not just the commercial component of it, I think, but the information that is being collected sometimes—it might be incorrect, it might be out of context; or it may be correct and in context, but lasts longer in the marketplace, if you will, than people might want it to, without the ability to explain it or to make up for some youthful transgression; or whatever it is that the information represents. And it could be meant for a specific audience and misunderstood if it's specifically, sort of, broadly distributed. And that can lead to harm, even to loss of job, loss of job opportunity.

Let's say, for instance, you had a cancer patient who communicates through a network—a support network of cancer patients. And somehow that enters into—with e-mail or reaches some other source, and it winds up becoming a source of herbal cures being sent to her, or some other kind of information that suddenly, sort of, tracks in. That may not be the way that cancer patient wants to lead their life. It may not be the way they want to be identified. It may be that their insurance rates go up because some of the information gets out to somebody. Maybe they'll lose a job opportunity, conceivably. But, who knows.

The bottom line is this. You know, we sat on this committee—I remember these conversations, 10 years ago, when Senator Hollings and we tried to pass a broadbased distribution of privacy rights. We couldn't do it. And we've learned a lot since then about, sort of, what happens. And I'd like to ask a few specific questions regarding some of that, if I may.

Let me just ask you, first of all, Professor Turow, What do you think about this "no harm, no foul" school of enforcement? Does

that do what we need to do? Does that provide a adequate standard by which we ought to live, here?

Mr. TUROW. As I was trying to suggest in my talk, "harm" is a very difficult concept. Sometimes, as you suggested, we can find harms. Sometimes we can quantify harms. I think the law would like to, historically, find harm that we can quantify monetarily, even. But, we're dealing with issues, often, of reputation, here. And we're dealing with, I would even argue, issues of respect and of social cohesion. So, I think we have to go a bit farther afield in looking at harm in the historical way that we've thought about it.

Senator KERRY. Well, let me see if I can pin that down a little bit. Mr. Taylor, at Facebook, you guys have crossed the 500 million users worldwide. And I think you've got more than 130 million in the United States. How many people at Facebook work on privacy issues and design?

Mr. TAYLOR. Everyone at Facebook works on privacy issues and design. Like security, privacy is a central part of our product planning and design process. So, during every aspect of the product's design and prototyping process, privacy is an aspect of discussion.

Senator KERRY. Is it accurate or inaccurate that, at Facebook, for instance, when a privacy concern mounts, or there's a modification of service somehow, that you change a practice that effectively can increase the amount of information that users share with others. Users then express concern about that, conceivably. You modify that practice somewhat, but the process sort of repeats itself. And it's a viral spreading of the same practice, in essence, the same gathering of information, even though there's a slight modification. Is that——

Mr. TAYLOR. Well, I just want to clarify one thing, that we have—we never retroactively have changed people's settings. There have been points where we have transitioned from one set of—I'll just give you one practical example, since this is somewhat abstract.

When Facebook started expanding from college networks to the whole world, there was no notion of—at the time, everyone signed up as a member of a university, and so we needed to expand that notion to beyond universities. So, we made networks for entire countries. So, everyone who joined from the country of Turkey joined the Turkish regional network. At some point, it became sort of a meaningless distinction, because sharing with the entire country of Turkey is roughly equivalent to sharing with everyone in the world. So, when we got rid of regional networks and we were modifying the way privacy worked on Facebook, every single one of our users went through a wizard that—where they got to choose the new setting, because, for example, that particular type of setting had gone away.

Senator KERRY. If you drop out or change your setting, does the old—is—what happens to the old information? How long is that kept?

Mr. TAYLOR. What do you mean by "old information"?

Senator KERRY. Well, if you change it, is it lost forever in your main depot of information, in your mainframe or whatever your storage mechanism is, or is it—I mean, you still can operate and use it?

Mr. TAYLOR. So, any information that you publish to Facebook, you can remove; and anytime you change a privacy setting to something, you can easily change it later, and it applies to all of the information you've published.

Senator KERRY. But, do you keep the—do you still have the information? Even though it's changed, in terms of the presentation on the Internet, on Facebook, do you have that stored?

Mr. TAYLOR. By "that," you mean the privacy setting? Or——

Senator KERRY. Whatever was there before.

Mr. TAYLOR. Well, absolutely, if a user publishes a photo to Facebook, we consider it an obligation to retain that photo unless they choose to delete it, because it's a user's photo and a meaningful part of their lives.

Senator KERRY. If they delete it, is it deleted from your storage?

Mr. TAYLOR. That's correct, yes.

Senator KERRY. It is. And all other information, likewise, if it got changed?

Mr. TAYLOR. If—we've tried to take a very proactive approach with privacy. Today, if you went to your Facebook privacy page and you set your privacy setting to "Friends Only," it would not only apply it to all future things that you share, but all things you had previously shared, as well. So, we've tried make it easy to not only—not only to enable people to change the—their privacy settings, but to enable them to change decisions they made in the past, as well.

Senator KERRY. Final question. I know I've gone over my time, but——

The CHAIRMAN. Go ahead.

Senator KERRY. Do you have the ability to cull from that information? Do you have the ability to, sort of—is there some formula by which you can commercially scan the information that's there and make some kind of determinations?

Mr. TAYLOR. Our exclusive focus at Facebook is the information users have explicitly decided to share on their profile. One thing that's fairly unique about Facebook is that it has been, from its inception, a service for sharing.

People put information in their Facebook profile because they want to share it with their friends.

Senator KERRY. I understand that——

Mr. TAYLOR. Yes.

Senator KERRY.—but do they want to share it with you in a way that you can, sort of, cull it and use it for various kinds of statistical analysis or broadbased breaking people up into categories and then putting them out and marketing something to them? Do you do that? Or can you?

Mr. TAYLOR. So, there are sort of two parts to that question in my head. One is—I just want to make sure it's clear—Facebook never sells data to third parties, and never sells data to advertisers, without question.

The other aspect is regarding advertising, I believe. The—clarifying that we never sell information to advertisers. Ads are targeted on Facebook only to the information you've explicitly put in your profile. And if you remove that information from your profile, ads will no longer be targeted to that. So, for example, I list Green

Day as one of the bands I like in my profile. That is something that—ads might be targeted on that information.

If I remove that, ads would no longer be targeted on that information.

Senator KERRY. Thanks, Mr. Chairman.

The CHAIRMAN. Thank you very much. It's a good line of questioning.

Senator McCaskill.

STATEMENT OF HON. CLAIRE MCCASKILL, U.S. SENATOR FROM MISSOURI

Senator MCCASKILL. Thank you.

I recognize that advertising makes the Internet work. I completely get that. And it keeps it free. But, I'm a little spooked out at the way this is developing.

Imagine how an ordinary American would react if someone took a camera and followed them around the store, videoing everything they were buying, watching them make selections between this makeup or that makeup, watching them make selections between this brand of soap and that brand of soap. There would be a hue and cry in this country that would be unprecedented, that somehow there were secret cameras following them around and figuring out what they're buying them, and then using that information to market them directly. And that's exactly what's occurring.

I was sitting up here, and I thought, just for fun, I would go and surf for something that I didn't really want right now. And so, I went on the Web and I looked up a foreign SUV. I'm not in the market for a foreign SUV. Frankly, if I were going to buy an SUV right now, it would certainly be an American SUV. But, then I went on another website, within 10 minutes of when I did that, and guess what ads were on that website. There were a bunch of ads for foreign SUVs. Now, that's creepy. That means somebody is following me around with a camera and following what I'm doing. And if this is taken to its logical conclusion, we could kill the golden goose, here.

And I would ask, especially those that—Google. I know you guys are using algorithms to read e-mails. And it's my understanding that you're doing it internally only. But, could you address the issue that I'm talking about, that you're reading e-mails internally and then using information, maybe not identified with anything other than a number, but, nonetheless, using the algorithms to predict marketing behavior.

Dr. WHITTEN. Certainly. So, this is a really good question. And I very much sympathize with this concern that people would have about the feeling of being followed. And I think it's a very, very important one for us to address.

Specifically in the case of e-mail, let me clarify that Google systems are not attempting to do any prediction of marketing behavior based on the contents of e-mail. What Gmail has always done, from the very beginning, was to take the same systems that scan an e-mail in order to identify, for example, whether it's spam and should go in the spam folder and the user shouldn't be bothered with it, to have those very same systems trigger off of keywords to show an ad that might be relevant.

And let me tell you about an example when I myself actually purchased something through a Gmail ad and had that happen. I was e-mailing back and forth with my mother, a couple of summers ago, a really, really hot summer. And she was complaining about the heat. And I offered to buy her an air-conditioner, in my e-mail. And as I was sitting there looking at the e-mail I had just sent, in Gmail, because it had the keyword "air-conditioner" in it, there was an ad for air-conditioner next to it. And, it was a pretty good deal, and I clicked on it, and I bought my mother an air-conditioner through that ad.

But, that ad was shown purely because that keyword was in that mail message I was reading right then, and that was a transient thing. That was not used to build any kind of profile of me as someone who has an ongoing interest in air-conditioners. It was purely something that happened in the moment right there.

Senator MCCASKILL. Well, let me ask this. Isn't it true that, at this point, there are coupons that you print out on the Internet, and you take them into a store, and you use them, and embedded in that barcode is a whole bunch of information about you? And do you think the consumer has a right to know that, that by using that coupon they, in fact, are aiding the marketing to them of additional things that they may not want and, frankly, that—I mean, don't you see that as a privacy issue that you need to address? Because I don't think most Americans get that's what's going on. I think when they print out a coupon, they think that barcode tells them—the vendor what the product is. I don't think they know that barcode tells the vendor about them.

Dr. WHITTEN. So, to be clear, this is not a practice that Google engages in. But, to your larger question, yes, absolutely, I think the challenge before all of us, and very much the challenge that I take personally and that my team takes personally, is to try to make these things not mysterious for people, because a lot of the distress, we think, comes from the fact that people experience these things as happening behind the scenes in a way that they don't have any control over.

And so, what we have really focused on, what we have really tried to do, is to find innovative ways to push that understanding of what's happening to the foreground, where it's visible to users in meaningful ways. And this is really what we were trying to do with the Ads Preferences Manager, especially by pushing for the in-ads notice, to have something in every ad, to build many ways to get the Ads Preferences Manager, to make that an engaging interface, so that hopefully people would actually want to look and see what interest categories were associated with their cookie, and to participate in editing it and taking some control over that.

Senator MCCASKILL. It's a little different—and I know I'm over on my time, and I won't go further with this—it's not as, probably, disconcerting to all of us, because we're used to people poking around our lives and trying to find things.

In fact, it'll be a great boon for opposition research, because now—I discovered this morning—my staff brought to me a printout—and I'm not going to use the name of the company, because I don't want to give them the press—but a company that, you can go on the Internet—and my colleagues would find this inter-

esting—if you want to pay them five bucks, they'll tell you a whole bunch of stuff about you. They'll tell you where you like to shop, they'll tell you where you live, how many bathrooms your house has, whether or not you're wealthy, how old your mother is. And so, for the folks out there that have been making a lot of money on opposition research, the Internet is going to be a big help to them, because they're going to be able to find out a lot more stuff, for five bucks, than they typically have—it's usually spent thousands of dollars on opposition research.

So, I don't know that all of us—I mean, we're kind of used to an invasion of privacy. We sign up for an invasion of privacy. We embrace it willingly. But, I do think that you all need to really address the phenomenon I'm talking about, because, as the American public catches on to this, they're going to be very unhappy.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

Senator Klobuchar.

STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Thank you very much, Mr. Chairman.

You know I started my day, just to follow up on what Senator McCaskill was saying, with Erin Andrews the ESPN reporter who had her images of her undressing in a hotel room distributed all over the Internet, as well as some other members of the House were sponsoring a bill to do something to improve our stalker laws so maybe they are as sophisticated as the predators who are violating them. And so, I hope all your companies will support these changes. I think it's going to pass the House today. But, as we know, the Senate always takes a little more time. And I think it'd be helpful to have the support of your companies, something that clearly goes beyond just your responsibilities, as predators involve, but the tools that are used by these predators: the Internet.

My first question is of you, Mr. Taylor, from Facebook. I appreciate the work that you're doing in the privacy areas. You know, I've raised a concern about having a—more accessible safety information on the Facebook pages, because, as I know from my 15-year-old daughter, who did all her birthday invitations on Facebook, a lot of young kids are using these—your number of even like 5-year-olds using is incredible. And if you could be—I know you have your "Privacy" button on there, I know you're working on this, but if there's a way to have a more easily accessible safety information, so kids know what to do if they suddenly get a request for a friend of someone they don't know, as opposed to having it a few clicks down. Could you respond to that, Mr. Taylor?

Mr. TAYLOR. Yes, absolutely. We recently launched a Safety Center, which is accessible from a fairly prominent part of our Help Center. And I think we, as a company, share your concern about safety, throughout the company. Like privacy and like security, it's something we think about with every product that we launch.

And I just wanted to highlight a few of the things I think are really important, because this is a really subtle issue. One of the things we've focused on is contextually giving our—the people who use Facebook the ability to report suspicious activity or offensive

content. And so, throughout the site there are links for people to report content that they either think came from someone who's either bullying or perhaps predatory in some way or any content that they feel is inappropriate.

I think that's a very—it's a very important issue that's not highlighted in some of the discussions I've heard, but it's important because, at the time that someone's experiencing something suspicious, giving them the ability to report that, and having our automated systems, as well as our operations teams, have as much information as possible to pursue these cases and disable accounts and, as it's relevant, report it to authorities, is very important.

The other thing is, I'm sure you're aware, but I just also wanted to highlight, we've worked with every single State's attorneys general to run their list of known predators against our accounts, disabling a very large number of accounts and reporting it back to authorities. But, the reason I wanted to highlight the report links is because that only goes so far. And we hold ourselves to a much higher standard than that. And having those inline report links is a very important part of maintaining a safe environment on our site.

Senator KLOBUCHAR. I appreciate that. And I just hope we can continue to work on this issue to see if there's a way we can just highlight those safety links so these kids know what to do, because these are just kids. And the more we can make it relevant, you know, with a button that says, "If you're," you know, "something's"—"you're worried about, scared about something"—"safety," as opposed to just "privacy"—I think that that would trigger them more to look at it. So, we can continue working on that.

Dr. Whitten, in May we learned that Google had inadvertently captured and archived private data from unsecured home wireless networks while compiling photos for the Street View map feature. After the incident I exchanged letters with your CEO, Eric Schmidt, and I'm glad that we're working together, moving forward. Could you talk about the outcomes of this—what I consider a serious privacy violation? And has Google conducted a thorough audit to ensure that other products and services do not contain unsanctioned code?

Dr. WHITTEN. So, we are still conducting our very thorough follow-up investigation. I, myself, am not a member of the team focusing on that directly, so I will be somewhat limited in what I can reply to.

We have committed to, however, when we have finished the investigation, to communicating publicly what changes we will make to ensure that this kind of mistake doesn't happen again. We take this very seriously.

Senator KLOBUCHAR. I appreciate that. So, that it's not an ongoing—it is stopped, but you're just figuring out how to change things so it doesn't happen again? Is that a fair——

Dr. WHITTEN. The——

Senator KLOBUCHAR.—characterization?

Dr. WHITTEN.—investigation is still underway.

Senator KLOBUCHAR. OK. Thank you.

One issue that isn't often discussed is peer-to-peer file-sharing and the privacy concerns that arise when kids use these programs.

We've had a number of unbelievable stories in our state, where someone who works at a gardening company goes home, does her company's business on the home computer, and doesn't know, but her kids has put a peer-to-peer file on there, and then all the company's data goes out onto the Internet, and they became victims of identity theft, their Social Security numbers stolen. Anyone want to comment about what we should be doing on this? Senator Thune and I have a bill to try to address it.

Anything? Peer-to-peer? No takers?

Oh, Mr. Harper, thank you.

Mr. HARPER. I'll take it up. I haven't been on a peer-to-peer network in a lot of years now, actually. What that really calls for most is, like everything we've talked about, better consumer awareness and better education. That's the hard way, but it's really the only way to get good outcomes like this. Good parenting, I emphasize again and again, which is not distinct from controls and things like that—good parenting is always right at the center of protecting children online. You're not going to——

Senator KLOBUCHAR. Right.

Senator HARPER.—come up with a magical technology solution beyond what parents can do.

Senator KLOBUCHAR. Well, as a parent who didn't even know, when I was running for office, what "LOL" meant, much to my daughter's embarrassment when I was asked the question in a campaign event, I don't think every parent can know everything about what's going on, and that's why I suggest you look at our bill, just because we're trying to give adults that—on that computer more information about what their kids have put on there, so that they can maybe stop it. And that's what we're trying to do.

I've got to step out for something, and I'll be back, Mr. Chairman. Thank you.

The CHAIRMAN. That was dramatic.

Senator KLOBUCHAR. As I always am.

The CHAIRMAN. Senator Begich.

STATEMENT OF HON. MARK BEGICH,
U.S. SENATOR FROM ALASKA

Senator BEGICH. Thank you, Mr. Chairman.

I just have a couple comments and question, but first, to Facebook, to Mr. Taylor. Could you—how do you notify, when you make these changes—you described this—the new safety security component—how do you notify your customers of this?

Mr. TAYLOR. There's a variety of mechanisms, depending on the magnitude of the change. So, on some——

Senator BEGICH. Let's start with the one where—the safety changes—security changes you changed. Or you might——

Mr. TAYLOR. So, I believe—my understanding, which I believe is—in—accurate, but I'm not directly working on this, so excuse any minor inaccuracies—is that we launched it to a prominent part of our Help Center, which is the central support part of the Facebook website. And we also launched ads, within our own ad system, to advertise the presence of this new center to our users.

Senator BEGICH. OK. And where would you label this one, in the sense of importance to your customers? In other words, would this

be the maximum amount of notification you'd make to your customer base?

Mr. TAYLOR. No. It's definitely not the maximum amount of notification. Some prominent changes to our service will notify with a prominent notice at the top of your Facebook home page, which is the entrance point to Facebook as a product, and by far the most important page on our site. And that's where we'll include information about significant changes to the user interface of Facebook or to other product launches that we think have a significant impact to the Facebook user experience.

Senator BEGICH. OK. Thank you very much.

Ms. Whitten, let me, if I can—I want to take that air-conditioning example, there, one step further, if I can. Once that company then sold you that air-conditioning unit, now they have data on you, correct?

Dr. WHITTEN. So, let me walk through what happened, step by step——

Senator BEGICH. Let me——

Dr. WHITTEN.—because——

Senator BEGICH. Let me——

Dr. WHITTEN.—I think that would——

Senator BEGICH.—pause you there——

Dr. WHITTEN.—be the clearest——

Senator BEGICH.—for a second, because I'm—I consider some of this like the catalog business on steroids. You know, you order one catalog; before you know it, it's 80 percent of your mail. So——

Dr. WHITTEN. Sure.

Senator BEGICH. So, now you've ordered—I want to take it from that point—you've ordered this air-conditioning. What happens to that data, that they have now collected, that took the phrase, or the words, "air-conditioning" out of an e-mail?

Dr. WHITTEN. So, first of all the air-conditioning company told Google it would pay to have this particular ad——

Senator BEGICH. Right, through association.

Dr. WHITTEN.—shown to that—right.

Senator BEGICH. Right.

Dr. WHITTEN. So, then I'm reading my e-mail, and my e-mail has the words "air-conditioner," and so, that triggers the system, and it shows me that air-conditioning ad. And then I click on that ad, and I am taken——

Senator BEGICH. To their website.

Dr. WHITTEN.—to that advertiser's website. At that point, thereafter, I am no longer dealing with Google. I am now——

Senator BEGICH. I see.

Dr. WHITTEN.—talking directly to the advertiser. And I put the air-conditioner in my shopping cart, and I give them my delivery address and my payment information, and the ongoing relationship that I might have with the air-conditioner company is established through that transaction.

Senator BEGICH. But, in essence, started with just "air-conditioning" in your e-mail?

Dr. WHITTEN. That's what triggered me being directed to the——

Senator BEGICH. Right.

Dr. WHITTEN.—to the air-conditioner——

Senator BEGICH. Yes.

Dr. WHITTEN.—company. But, they had no information to pursue an ongoing relationship with me, until I went to their site and——

Senator BEGICH. Understood.

Dr. WHITTEN.—interacted——

Senator BEGICH. And you——

Dr. WHITTEN.—with them directly.

Senator BEGICH.—made a commitment at that point, at whatever that level was. Did the Website say to you, when you purchased the air-conditioning unit—I mean, the assumption is, because you're in the industry, that the minute you do that, you're going to get a lot of stuff from them. Will that——

Dr. WHITTEN. I don't remember, for that particular air-conditioner company. I must say, I don't actually remember getting a lot of air-conditioning-related——

Senator BEGICH. May not be air-conditioning company, but——

Dr. WHITTEN.—solicitation e-mails afterward.

Senator BEGICH. But, I mean, the assumption——

Dr. WHITTEN. So——

Senator BEGICH.—is that, once you go on there——

Dr. WHITTEN. Yes.

Senator BEGICH.—it asks for your e-mail and all kinds of stuff to confirm the order, that you're in their system.

Dr. WHITTEN. Yes.

Senator BEGICH. Is that a fair assumption?

Dr. WHITTEN. I mean, my experience, as a consumer is that industry practices, generally—they're sort of an opt-in/opt-out, too, "Can we send you more promotional e-mails?"

Senator BEGICH. What—for the companies that are here, what more—what one thing would you recommend, if any, that should be done to increase the level of security and privacy to the users of your facilities? I use "facilities" in broad, because one's AT&T, one's Google, Facebook. But, I mean, what's the one thing that should be improved? Because I'm not—have you—tell me you're doing it all right, I'm going to——

Ms. ATTWOOD. Well, let me——

Senator BEGICH.—the——

Ms. ATTWOOD.—let me comment on that.

Senator BEGICH.—the radar will go up, and that won't really be a good answer. So——

Ms. ATTWOOD. So, what's remarkable in this hearing——

Senator BEGICH. I'm trying to be very polite.

Ms. ATTWOOD.—is for all of us to acknowledge or address the fact that we believe we're "best practices" in the industry. We're adopting the notice-and-consent framework that the FTC talked about; we are, in fact, innovating in the way in which we're talking to our customers. But, the one thing that's missing is that we're not, in fact, honoring each other's customers' permissions. So, every day there are literally millions of customers who use AT&T's service on Apple's iPhone to go to Facebook and check their friends' status, and then go to Google to check on where they should meet for dinner. That happens millions of times every day.

That customer, in order to understand where their information has gone, has to read all of our privacy policies. And, I—you know,

I'm very proud of our policy. We've worked very hard to make it very secure and very clean—very straightforward to the customer, but there is nothing that, in fact, gives the customer who—comes to AT&T and says, I want to have my information protected. I, in fact, can only do what I can do with AT&T. I can't, in fact, honor that across all of my partners who are here.

And I do believe that's the next phase of what we have to do when we think about demystifying it for the consumer, making it less creepy. We have to, in fact, work as a industry, as we're doing, and push the boundaries of saying, when somebody says to me, "I want my information protected in a certain way," or says to Google they want their information protected, I honor that, Google honors me, and we give a single unified face to the customer, in terms of their permissions.

Senator BEGICH. Very good.

Mr. HARPER. Senator, can I interject with one thing that I don't think companies would probably want to bring up. That's the idea of individual consumers exercising control over cookies. We talked about it a lot. Cookies are the primary way that you're tracked from site to site——

Senator BEGICH. Right.

Mr. HARPER.—usually on ad networks or that kind of thing.

Senator BEGICH. Right.

Mr. HARPER. In both Firefox and Internet Explorer, the most popular browsers, you go to the tools menu, select options, click on the privacy tab, and you can decide whether you accept cookies from no site at all, or the sites—the primary site you're visiting. You can deny third-party sites, which are usually the basis for tracking.

Senator BEGICH. Right.

Mr. HARPER. I'm a little bit of a stickler. I look at every cookie coming onto my computer, it doesn't take too long once you're into it. But, people can create blanket rules about that kind of tracking and put a—take a big chunk out of the kind of tracking that Senator McCaskill was worried about. That's the one thing that consumers can do that'll put them in a good position.

Senator BEGICH. And I know my time's up, so let me—I'm sorry, Mr. Chairman——

Mr. TUROW. I just——

Senator BEGICH.—maybe you want——

Mr. TUROW.—quickly want to add, while that—I think you're absolutely right about that. It has to be said that, increasingly, companies are trying to get around cookie problems. Just, as you say—companies are beginning to use first-party cookies because they knew third-party cookies are zapped. Toolbars can be used without any cookies at all. And, as people know, there are some things called "flash cookies" that don't extinguish.

[Laughter.]

Mr. TUROW. There are lots of ways—registration. The industry knows that cookies are sometimes fallible and in danger, and there are ways that people are trying to get around them.

Senator BEGICH. I apologize, Mr. Chairman, I exceeded my time.

The CHAIRMAN. Thank you, Senator Begich.

Dr. Tribble, I'm afraid that, one, you feel you're being ignored, and second, I've stolen——

Mr. TUROW. No. I'm not being ignored.

The CHAIRMAN.—something from you.

Dr. TRIBBLE. What was that?

Mr. TUROW. The—oh——

The CHAIRMAN. So, I want to tell you——

Dr. TRIBBLE.—that's his.

The CHAIRMAN.—that it's still here.

Dr. TRIBBLE. OK.

Mr. TUROW. That's his.

[Laughter.]

Mr. TUROW. Mine's in my pocket.

Dr. TRIBBLE. Thank you.

The CHAIRMAN. But I want to—oh. Did—was that yours?

Mr. TUROW. No, that's his.

Dr. TRIBBLE. Yes.

The CHAIRMAN. That's his. Yes.

Dr. TRIBBLE. Yes.

The CHAIRMAN. I wanted to make a point from it, because it makes a point for me. You indicate—now, let's say I'm a 55-year-old forester from central Montana. And you indicated that all they have to do is go to the particular "click" and then they'll get their capacity to protect themselves.

It turns out that on your machine here, the particular click is labeled "Settings." And I'm trying to figure myself coming down out of the top part of a tree and finally reaching the ground and running and getting this, that if I go like this—in theory, I get what you gave me and I get my choice. But, on the other hand, I had to go to that "Setting." What does the word "Setting"—how is that meant to mean something, not just to a—somebody who's cutting up trees or mining coal, but, as Senator Klobuchar said, to some 13-, 15-year-old kid?

In other words, to you it's very clear. And one of the things that interests me in all of this is that there's total clarity with all of you, and total certainty. Occasional mistakes. But, to the rest of the world—and I am going to have somebody return this to you.

[Laughter.]

The CHAIRMAN. Keep my reputation intact. But, it isn't all that clear. And I think that's a hard connection for somebody to make. I wouldn't go from—you know, to "Settings." I'd look at all the other things—clock, time, weather, sports, stocks—and maybe I could eliminate, if I spent time on it, getting down to "Settings"—"Well, maybe it's here," push it, get what you want. But, see my point?

Dr. TRIBBLE. I see your point. And I actually agree with your goals of clarity, and I can tell you that we strive for that, in terms of the usability of our devices. And finding things like this easily on a device is a challenge. It's something that we try and excel at, actually.

One of my points, about this particular feature, was that it's important that privacy issues not just be relegated to a privacy policy, that they actually be designed so that they're part of the user interface that the user would encounter normally during the use of their

device. And, you know, we may not have reached perfection there. I don't think we have. In fact, I think, more innovation is actually required in this area. It's a simple fact that not every particular feature, including privacy, can be at the top level, one click away from the home screen, or things actually get back to being so complex that it's hard to deal with them again.

So, making the decision where in the user interface should the privacy issue be—we think it's very important. As I mentioned, if your location is being tracked, we actually went ahead and took space next to the battery indicator to go ahead and put an icon right there, that's always showing you, Is your location being tracked? We think that's at least—if not more important than how much battery you have left.

Integrating this into the user interface is one of the areas where we're actively innovating. I think there's more innovation yet to be done there.

The CHAIRMAN. I do, too.

Dr. TRIBBLE. So, I agree.

The CHAIRMAN. I'm going to—Dr. Whitten, I'm going to say something not entirely pleasant to you, but it surprised me that you're in charge of security and, you know, openness for Google, and you start out with a 3-minute lecture on how much money Google makes, how huge it is. We all know that. So, psychologically, I'm sort of interested, why did you start out on that? I don't need to have you answer, unless you want to. But, I just want to say that for the record. It was interesting to me that you started talking about how successful Google is.

You have nothing to say, so I'm going on to Mr. Taylor.

Mr. Taylor, your privacy policy has the following: quote, "Even after you remove information from your profile or delete your account"—this gets back to Senator Kerry—"copies of that information may remain viewable elsewhere."

And then, it goes on to say, quote, "Certain types of communications that you send to other users cannot be removed, such as messages," which are kind of basic.

Now, it sort of begs the question, if the Facebook user wants to permanently—and this is what Senator Kerry asked—to delete—and you gave him a very firm answer, "It's gone." This says otherwise.

Mr. TAYLOR. I just want—I'm sorry, are you done? Would—is it an appropriate time to answer?

The CHAIRMAN. Yes. Go right ahead.

Mr. TAYLOR. All right. I think it's a very good point. And you bring up some of the most subtle issues that we'll deal with in working on a social product.

The issue about, "Your data may still be viewable elsewhere," it's an important point to just give our—the people reading that policy a realistic expectation about how information may flow throughout the Internet.

So, for example, you may publish your phone number to your Facebook profile. And your friend might take that number and copy it into their phone, that interaction came from Facebook, and, even though you deleted your Facebook profile, that copy of that information may continue to exist because your friend copied it into

their phone. Likewise, your friend might take a photo that you published to Facebook and print it out and put it on a collage or put it on their personal home page because they copied it off of Facebook.

And, you know, when you're sharing information with other human beings on the Internet, you know, it's not just a technical thing, it's a social thing. And people may choose to do things with that information outside of the bounds of the things that we can control. And I believe, if I'm recalling the part of the policy you're talking about, that's specifically the realistic expectation that we are trying to make sure people using our service understood.

Regarding, "There are some pieces of information that can't be deleted, like messages," we thought a lot about this, and a lot of people use our messaging product much like they use e-mail. And when you send someone an e-mail you don't have the ability to delete it from their inbox. You've sent it to them. Just like once you've sent a letter to someone and it ends up in their hands, you have the social ability to ask for it back, but, you know, at that point, it's in their hands. And when you send someone a message, we consider that piece of information, at that point, owned by two people, just because it abided by the existing conventions that existed with e-mail and even postal mail.

And so, those are very specific instances. Certainly, the information that you've shared on your profile is information you can delete permanently. And I think, in those particular instances, we were just trying to take a thoughtful approach that abided by the people who use Facebook, their expectations of the service.

The CHAIRMAN. Is it not true that somewhere—and this applies to intelligence agencies, too—that there is some point at which there is a residual place of keeping information that cannot be deleted under any circumstances?

Mr. TAYLOR. So, I can't really speak to what our intelligence agencies do. I can tell you that——

The CHAIRMAN. I'm not making it—the point out of the intelligence agencies. I'm asking that to you.

Mr. TAYLOR. Is there—do you mind clarifying your question? Are you asking, Is there—certainly, on—from our servers, when you delete your account fully, we delete all of the information associated with your account.

The CHAIRMAN. So, there's no backup anything anywhere which retains that.

Mr. TAYLOR. Certainly, these technical systems are complex, and there may be backups of some pieces of information somewhere, due to the complexity of these systems.

The CHAIRMAN. What if you're subject to a lawsuit and you have to defend yourself, and there's a lot of money at stake, and you have to go back and pull out that particular e-mail, whatever it was. You have to be able to do that, don't you?

The CHAIRMAN. You just say, "Well, I'm sorry. We can't defend ourselves."

Mr. TAYLOR. So, you're talking about if someone has deleted their Facebook account, what mechanisms we would have to look up that information of the deleted account?

The CHAIRMAN. Yes.

Mr. TAYLOR. You know, some of this may get into very specific details of our infrastructure that I'm not intimately familiar with. Certainly, the spirit of the account deletion feature on Facebook is that your information is deleted. As I mentioned, these technical systems, due to the technical requirements of making a system that's extremely reliable and available at all times of the day, may mean that there are backups and archival forms of this data in some parts of our system. So, I think that is a reality that—so, I'm not sure, in that specific instance, what information would be available.

The CHAIRMAN. And then, I move from my person, who's high up in a tree cutting off branches, to a 13-year-old, who is vulnerable, is lonely, is socializing. The—Senator Klobuchar making this point—and the ability to—for a predator. We've had hearings on this subject, too. And I do a lot of roundtables, in my State of West Virginia, about precisely that subject, the vulnerability of students, the vulnerability of young people. They are your future; they are your present. I don't know how much of your profits come from them, but a lot. And when I asked—when somebody asked you the question, "Who's responsible for privacy protection?" and you said, "Everybody who works at Facebook is." Everybody who works there is. And I found that somehow suspicious and disingenuous, because I think companies have to be divided up in certain things, and people don't spend all of their time on every single question that comes before them, saying, "What are the privacy consequences of this?" I don't believe what you said.

Mr. TAYLOR. I think that's a very fair point, Mr. Chairman. What I intended to say is that the engineers and product managers who are developing the products at Facebook take into account privacy in every aspect of the product design. We do have a team devoted exclusively to security——

The CHAIRMAN. I'd like——

Mr. TAYLOR.—and safety.

The CHAIRMAN. And I accept that.

Mr. TAYLOR. Yes.

The CHAIRMAN. But, don't you think there's the possibility, here, of beginning to divide the world into—and users—into two categories, those who know just exactly what to expect and how to handle themselves, what the consequences are of what they do—I'd put that group at 50 percent—and then others who are simply thrilled to be on Apple, on Facebook, on Google, whatever, and—but they're not really quite sure what they're doing? They're not sure of the consequences of what they do. They don't know what it means to be following them around, in terms of identifying their location. They're innocents. But, they're seriously into it. And it seems to me that we're almost dividing ourselves into two worlds.

You've got the world working for you, because you're making a—you're being tremendously successful, and people are signing up like crazy. And so, why complain? But there are consequences. There are inherent consequences. You know, the bullying thing, that was casually mentioned here, is not inconsequential. It's huge. Sexual predators is huge. And it's a part of what you do.

Now, if you can defend yourself against this, and if you go to the right clicks and the right icons, and do all—make all the right

moves, I suppose you can stay out of trouble. But then, always lurking is the record. People—you know, people are tracking you.

I didn't mean to leave out AT&T. I apologize.

You're being tracked. People are using you to advertise. The word "air-conditioning" did come up for a certain reason. And it was very convenient, in your case, because you were trying to help your mother. In other cases, it might not be so convenient, or it may even be confusing.

So, my philosophical question—actually, I aim at you, professor, this question, the question of, Are we dividing ourselves into two classes of people, people who understand it and who can handle themselves in this world, on all of these instruments that we have now before us, and those who cannot? And those who cannot are paying a price, which we do not yet fully understand, but which we're beginning to understand, and that does get into the abuse, and sexual this, and predator that, and bullying, and all the rest of it; or misinformation; or simply being marketed.

I mean—you know, it's the same question of—I mean, Senator Kerry and I get, frequently, telephone calls at our home, which are meant to be unlisted numbers. And somebody proceeds to grill us with a whole series of questions about something. You just hang up. That's an annoyance that should not occur in American life, if you don't want it to happen, but I have no way of stopping it. Hence, to the question, Can I really stop Facebook from having records on me? You say yes. I'm not so sure. In fact, I think not.

So, what do you say, professor?

Mr. TUROW. Well, there are lots of——

The CHAIRMAN. And the larger question is, Are we becoming two different societies, and isn't that wrong on something which is this dominant in our culture?

Mr. TUROW. I think we're becoming multiple-level societies, for a number of different reasons. I'll make it quite short.

One is exactly what you say, the people who know and the people who don't know. Increasingly, as I get into the data that we've dealt with, and that other people have done research on—I used to believe that a lot of these problems could be solved by education. I no longer believe that everything can be solved by people learning. It's much, much too complex. I find that professionals in the field, when I call them to check on things I'm thinking about, will not know the answers.

Reading privacy policies is becoming a scavenger hunt, because not only do you try to read the privacy policy and make sense of verbiage which is basically understood by the people who create it and not many others, you're also into links that send you to links that tell you that other parts of this are related to other companies. And they use words like "affiliates," that most people wouldn't understand. So, at that level, we have people who—I would say even very intelligent people couldn't make sense of that.

On another level, I'm concerned that we're moving into a world—and this gets us into television, not just what we call the Internet, because the television is going to be the Internet. IPTV, digital TV—we're going to have a situation where people will receive views of the world based upon what others know about them, and what they don't know others know about.

So, it's quite possible—and I've spoken to people now who are beginning to think about, for interesting reasons having to do with marketing—of changing the news profile you get, based upon the particular parameters that people know about you and, as a consequence, that will put people into certain kinds of, what I might call, "reputation silos." We're not there yet, but we're defining people's reputations in ways that they don't understand.

So, there are multiple levels relating to status, relating to education, relating to so many things, that I'm beginning to despair that we can ever really understand it. And that's why I'm beginning to think that some parts of this have to be regulated. Not everything, by any means. But, there are some issues that people will simply not be able to contain, themselves.

The CHAIRMAN. I'm so wildly over my time, it's embarrassing.

Senator Kerry?

Thank you, all of you.

Senator KERRY. Ms. Attwood, can you share with us what the recent glitch was about that saw the distribution of more than 100,000—I guess they were the iPad owners' e-mails?

Ms. ATTWOOD. Sure, I'd be happy to.

We had an incident recently in—that was largely called a "brute-force attack." It was a security breach by a—some hackers who were trying to collect information about iPad users. It was an incident where they—the hackers developed—looked at—developed software in which they would—used to capture e-mail addresses that were able to be captured on a Website, or actually on the Website that they pinged, because there was a certain—well, the—for the ease of the customer, the Website that they went to retained information about the e-mail address using the ICC ID code, which is the serial number of the iPad. And by writing a code, they were able to randomly seek to capture the information of that e-mail address, and constructed a list of those addresses.

We found out about the security breach when a media outlet said that the hackers had gone to them and proposed that there was a vulnerability in the security of the e-mail address. And within 24 hours, we fixed that vulnerability. Then we tried to assess whether there was additional vulnerabilities. We concluded that, in fact, the only information that was potentially vulnerable was the ICC ID code as well as—which is that serial number on your SIM card—as well as the e-mail address, and, in an abundance of caution, we notified all the purchasers of the iPad 3G device that there was a potential exposure of their e-mail address.

To date, though, I want to say, we have not seen that information be released in any other way, other than to these media outlets. But, we're cooperating with the criminal investigation that is looking into seeing how that security breach occurred.

Senator KERRY. How often do you guys get attacked like that?

Ms. ATTWOOD. It is a daily event that there are——

Senator KERRY. Is that true for all of you? Google, daily event? Facebook?

Ms. ATTWOOD. We spend millions of dollars on hardening and securing the network. It is a constant—there is a—it is almost a sport, in trying to expose vulnerabilities, as it is for the Federal Government, as well.

Senator KERRY. So, how is it that people who have their information trusted to you—entrusted to you—what kind of confidence can they have?

Ms. ATTWOOD. Oh, I think that developing the confidence, and maintaining the confidence of the security of the network, is absolutely essential. And in this instance, we were really disappointed. We spend literally millions of dollars establishing very secure networks, and, in this instance, we failed our customers. That's why, in fact, we—as soon as we understood the nature of the problem, we fixed it, and we notified them. We also have, you know, made available new SIM cards, if our customers feel that they need them. We don't think—you know, from a security perspective, we don't think that they're necessary, but we've also made that available. So, absolutely, it's—you know, they demand and expect more.

Senator KERRY. I think—you're an engineer, aren't you?

Ms. ATTWOOD. No, I'm a policy person. I—sadly, on this panel—so——

[Laughter.]

Senator KERRY. Well, can you tell me—are you able to tell me where in the system there's the greatest vulnerability and potential for abuse? Where in the networks?

Ms. ATTWOOD. Where in the networks? I mean, I think you have multiple areas that are capable of security violations. So, you have databases that—where you store information; you have physical links where, in fact, there—individuals try—you have devices where there are actually efforts to corrupt devices. So, in—I would describe, in the entire, you know, product line, you have multiple areas where you could see security breakages. And, in fact, we have, you know, a lab that is set up just to try to ferret out where those breakages could occur.

Senator KERRY. Can you tell us what "deep packet inspection" is?

Ms. ATTWOOD. Well, "deep packet inspection" can mean a lot of different things, but, essentially, it is the ability to read beyond shallow—every bit has a—certain information. Some of it is considered shallow information, kind of like addresses, and other portions of it are called "deep packet," which is payload information. It's the content of that bit.

And "deep packet inspection" is a—is the capability to evaluate the shallow and deep information contained in that bit. It's used, in our network, for trying to find malware—spyware—for purposes of network security. And——

Senator KERRY. Is it used for any other—is it used for any commercial purpose?

Ms. ATTWOOD.—thank you for saying so, because I heard the previous testimony. No, we do not use deep packet inspection for marketing purposes, which was the subject of the NebuAd interest a couple of years ago.

Importantly, I would also tell you that we have gone so far as to, in our privacy policy, explain that we will not use it, absent express permission of the customer. In the event that there seems to be a desire for the use of that information, we'd ask our customers first. So, no.

But, we do—deep packet inspection, like any technical advancement—and I would say, you know, all of us have had—there have

been discussions about recent issues that have been faced by companies on this panel, and each one of those involved the use of technology inappropriately. And so, in this context, deep packet inspection—I don't think there is anybody who suggests that that is not used appropriately when it's in finding and ferreting out fraud and abuse.

Where the issue was, was the use of that in a way that seemed to offend customers' and users' expectations. And because of that—AT&T was not doing that, was not planning to do that—but we went so far as to make clear we would not do that without our customers' permission.

Senator KERRY. Mr. Taylor, in response to the Chairman's question about the deleting of information and the storage of information, you repeatedly said that if it is deleted, it is gone. What if somebody simply deactivates their Facebook page? It's there forever, isn't it?

Mr. TAYLOR. So, I may get some of these details wrong, so—but, I'm basing this on my understanding of it. When you deactivate your Facebook account, for some period of time, you can reclaim it. It's—often people will—it's actually very frequent that someone might choose to disable their account at some point and then want to restore it at a later point. So, we added that as a feature to our users, at a point where we noticed a lot of people sort of had buyer's remorse about the decision to delete their account. People buildup a——

Senator KERRY. What's the——

Mr. TAYLOR. I'm sorry for interrupting you.

Senator KERRY. What's the point? I mean, at what point? How long?

Mr. TAYLOR. I don't know, off the top of my head?

Senator KERRY. Do you know, if they don't? So, you don't know whether or not it stays for several years.

Mr. TAYLOR. I don't think it does, but, because I'm not intimately familiar with the details, I'm uncomfortable giving a specific answer.

I think it is worthwhile to provide just a—one specific bit of context. The—people publish a lot of information to their Facebook profile. I recently had a baby, for example, and a lot of my baby's initial photos are in there, and the act of deleting all of that is a very significant operation. Just like there shouldn't be, you know, a button that deletes all the contents on your laptop's hard drive without, you know, a fair amount of deliberation; that's really the motivation for that particular piece of functionality. I just wanted to provide that context.

Senator KERRY. Fair enough.

Well, I—as everybody here knows, our counterparts in the House have introduced legislation, and I—we have sort of a cross-jurisdiction in this committee, with Senator Pryor and myself, the Consumer Protection Subcommittee and the Communications Subcommittee. So, we're going to work with the Chairman and—with the goal of trying to build the record. We've got these reports coming out, obviously, from the Commerce Department and the FTC. We'd like to work with all of you. I mean, the key question is, can we come up with a standard, some kind of a set of expectations

that are more effective? We struggled with this 10 years ago, and I guess it failed because we—you know, the offline/online sort of debate—and we got caught up in that, and tried to reach, maybe, too far at that point in time.

I think—incidentally, I think a—you know, I'm not suggesting your companies have not made differing and significant kinds of initiatives to try to respect people's privacy. And I think, all in all, the opt-in/opt-out debate that we were all worried about has been resolved pretty effectively, and I give you all credit for that. And I—but, you know, it's tricky. That's a long page of, you know, complicated conditions, and, you know, most people just zap down to the "I Agree," and they punch the "I Agree," and off they go. And so, I'm not sure that there's, you know, knowledge in the "caveat emptor" component of all of it, et cetera. And I think we ought to figure out if we can get a baseline here, where it's simpler and more direct. And I think that's the kind of thing we really have to work at. So, we certainly look forward to it.

Mr. Chairman, thank you for the lenience on the time, I appreciate it, and my colleague. Thank you.

The CHAIRMAN. Go ahead.

Senator KLOBUCHAR. Thank you very much, Mr. Chairman. Thank you.

The day is getting late here, and I had a few additional questions for you, Dr. Tribble, just about the subject that Senator Kerry just raised about the opt-in/opt-out. And you said, in your testimony, that customers may opt-out of interest-based advertisements by visiting, is it, *oo.apple.com*? Right?—"OO," not for double-agent–00, but for opt-out. And how do your users learn about opt-out? Because I think that's one of the things we're trying to figure out as people get these, you know, small-print policies. They're looking up on the computer, and they're trying to figure out what to do. How do they learn about the opt-out?

Dr. TRIBBLE. Yes. In this case, the opt-out link is, in fact, in our privacy policy document, which is linked to from every page on our Website. And, you know, we work hard, actually, to try and make sure that our privacy policy is in as plain English and is not lengthier than it needs to be. And, you know, we think it compares pretty favorably with other privacy policies that are out there. But, that is currently the mechanism.

I should point out that, in the case of iAds, that is something that we are just starting to do. In fact, we just started, earlier this month, to enable iAds on—which are ads that come up in the applications that you run on your iPhone. And, you know, that mechanism may evolve over time as we, perhaps, innovate new ways to, as I mentioned before, incorporate the control over a user's information into the user interface itself, rather than just relying on the privacy policy.

Senator KLOBUCHAR. Well, in your testimony you also indicated that your customers have an opt-in model for location-based privacy disclosures when using third-party applications, but they have an opt-out model for location-based privacy disclosure to Apple. Is that right?

Dr. TRIBBLE. I think what you said is correct.

Senator KLOBUCHAR. You can clarify it later if you want, in writing, or for the record. I'm just trying to figure out how a uniform opt-out privacy disclosure policy would affect Apple, if, you know, we were to mandate that, or something like that.

Dr. TRIBBLE. Well, with respect to location, as I mentioned previously, there is a master on-off switch for location-based data, so that the user always has the option of completely opting out from any location data collection at all. As Chairman Rockefeller pointed out, perhaps that could be at a more easy-to-find place in the user interface. But, that is the goal of that feature.

Senator KLOBUCHAR. OK.

And again, with—Dr. Whitten—with Google, along these same lines, about trying to read privacy policies when people aren't looking at everything—and we all know that—you might even have data on that, I don't know—how many of them actually read them.

Could you talk about how your users learn about Dashboard, and how do you inform them of the privacy options and what work you've done in this area?

Dr. WHITTEN. I'd be delighted to.

So, we've sort of developed a bit of a pithy saying as we try—internally—as we try to make progress on this, and this is to say that, you know "Show is better than tell, and show-and-tell is better than show." Right?

So, I—my perspective on this is that privacy policies are necessary, but they're only a beginning of the efforts that we should be making to try to explain, consistently, the same important things that our users need to understand about their privacy, in many different ways. And this is why at Google if you click the privacy link, you will go, not just to a privacy policy, but to a privacy center, which contains the privacy policies, but it also contains frequently asked questions. It contains things like, for example, when we were first launching Chrome, we commissioned a comic book from a famous artist, to explain some of the things about the way Chrome worked, and the controls that we had built into it. It contains YouTube videos of me and others explaining aspects of how Google uses data, what controls are there, and how the Dashboard works.

So, all of this is, I think, a really important component of trying to present that same information many, many different ways, so that people will have a good chance of finding clear explanations in the way that's most accessible to them.

But, another component of it, and one very dear to my heart, is working to build the clarity of what's going on, right into the experience of the product. And again, with the Google Dashboard, it was very important to us to make that be, ideally, something that people would go to just because they wanted to know, "Where's all my stuff?" That it would be like going to your desktop, almost. And that, because the Dashboard presented in this, "Here, this is just useful, in a practical way," a view of what all of the information stored in the account was, and what the options are, people would be consciously aware of that, even if they weren't thinking privacy, privacy, privacy. We didn't want people to first be concerned, and then click through and see things. We want to find ways to really put it in front of them.

And, you know, I think there's still a lot of work to be done, there's still a lot of mysteriousness to be cleared up, and hopefully that'll keep my team busy.

Senator KLOBUCHAR. And I know that the Chairman had asked you about your testimony in talking about the—Google and how you've grown, and I was thinking about that—that question some. And I think one of the messages that we all have for you is that you have been very successful, and we appreciate that. We appreciate the jobs that you have brought, all of you, to our country, in this development, here.

But, with that growth comes responsibility for piracy—privacy—and as well as warding off piracy, may I add, Ms. Atwood. But, this responsibility for privacy of these things that we just wouldn't imagine people are trying to do to steal things, and predators getting information. And that's what I think you're hearing from all of us today, is what we hear from our constituents, of experiences they've had. And I know you've heard them, as well. But, it's our duty to be here to say, "We need to do something better here." And you know some of it's going to be enacting laws, and some of it's obviously going to be things that you all do.

So, I want to thank you for your testimony, and we look forward to continuing to work with you as we draft laws and try to do the best thing for the people of this country.

Thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Klobuchar.

I don't have a question, I just have a closing thought.

I remember 10, 15 years ago—when was Y2K? When was that? Ten? Cato comes down with 10. Do I have a 12?

[Laughter.]

The CHAIRMAN. And what was fascinating about that, and what is sort of on my mind, is what an unbelievably naive display that was of an enormous number of very large jets coming in, the day before a vote, to land—as you could then do at the Washington Airport—and Senators, right and left, were summoned into absolutely cannot-miss meetings to tell us what the stakes were, and how we should vote—the next day.

And I—that's still very much in my mind. And it describes, I think, the separation, in some respects, between your world and our world. It's not just a matter of Silicon Valley, East Coast, those horrible people in government.

But, there's the unfortunate fact that we do have oversight over you. And this is hard for you to live with, because you're off on a tear, doing great things for this country, and Senator Klobuchar and I are left with incredibly frustrated parents, principals, school board members, police officers, coming and complaining to us, on a regular basis, about the fallout of what it is that you do. And I don't say that with hostility, I say that with a sense of—that we each have to reach out to each other.

But, you should know that this committee—it's called the Commerce Committee, and I've been on it for 26 years—we've changed. And we've changed much more into a consumer- protection type of committee. We find ourselves up to our ears in scams, and pop-ups, and what the health insurance industry did all during the

healthcare debate, the way they finally were taken to court, and we had to let—deal with that, and how they're still trying to take the medical loss ratio, which we finally had to pass when the public option couldn't pass, and they're trying to twist that before Health and Human Services can put out a final ruling on it.

I mean, aggressively, people trying to shape the world the way they want the world to be. That is behavior which I can fully forgive, provided there is a counter on the other side. The other side, in this case, happens to be us.

You've heard some very, very bright people, with some very passionate thoughts, and some very deep reflections on the success of your industries and the use of your industries by all of us.

But, there is, as Senator Klobuchar said, the other side. And that's where we use words like—that's—Dr. Tribble, that's why I pointed that thing out; I made myself into a coal miner, a tree-climber, something of that sort. But, it was right to do so, because that's what most people are like in this country—in the East, the Midwest, the Southwest, the Northwest, and California.

And so, I just hold that out as a thought for you, that we're doing this together, and we are—the people who sit behind us on these things are incredibly sophisticated wizards at what you do. And if we're going to make American better, if we're going to protect children, we're going to protect—cause parents to do as much as they can to be responsible, but understand when they can't be, because they just don't have the time—they're dead tired, they're on their third job of the day, whatever it is—that, still, this—all of the system has to work.

You started out the day, it seems to me, just a bit—talking about "We are all about privacy protection online." And it ended up a little bit more, "Well, we still have a lot to do. We have a long way to go." And there were things that came up, which I didn't find—what—didn't find satisfaction in, but found interest in, to simply say, in closing, that we need each other. But, it's important to understand that you need us, too. Because we represent the American people in ways that you do not. They do more business with you, but they depend upon us. So, we have our work to do, all of us.

You're terrific to be here, and to stay this long. Most wouldn't have done it. But, you did get your machine back.

[Laughter.]

The CHAIRMAN. Thank you all.

[Whereupon, at 5:38 p.m., the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF LAURA W. MURPHY, DIRECTOR, WASHINGTON LEGISLATIVE OFFICE AND CHRISTOPHER CALABRESE, LEGISLATIVE COUNSEL, AMERICAN CIVIL LIBERTIES UNION

Chairman Rockefeller, Ranking Member Hutchison and members of the Committee:

On behalf of the American Civil Liberties Union (ACLU), a nonpartisan public interest organization dedicated to protecting the constitutional rights of individuals, and its more than half a million members, countless additional activists and supporters, and fifty-three affiliates nationwide, we applaud you for turning your attention to the important question of consumer online privacy. The ACLU has long been concerned about the growing collection of personal information by private entities. In our 2004 report "Surveillance-Industrial Complex: How the American Government Is Conscripting Businesses and Individuals in the Construction of a Surveillance Society" we wrote about the widespread collection of information by the private sector.[1]

To identify the policy issues related to consumer interactions with corporations and other private parties, it is crucial to understand the larger context of information sharing throughout our society, including sharing with the government. Rapid technological advances and a lack of updated privacy law make information sharing between private parties and the government easier than ever, which in turn means that privacy invasions from the private sector can quickly become privacy invasions from the security agencies as well. This broader context must be considered when policymakers form judgments about the risks and benefits of sharing personal information and establish necessary protections to safeguard online consumer privacy.

This statement includes a brief description of this problem and two concrete measures—data retention limits and bars to third party access to personal information—that the Committee can take to limit it.

Background

Acting under the broad mandate of the so-called war on terrorism, the U.S. security establishment is making a systematic effort to extend its surveillance capacity by pressing the private sector into service to report on the activities of Americans. That effort colors all discussions of privacy focused on the private sector.[2]

Public-private surveillance is not new. During the cold war, for example, the major telegraph companies—Western Union, RCA and ITT—agreed to provide the Federal Government with copies of all cables sent to or from the United States every day—even though they knew it was illegal. The program, code named "Operation Shamrock," continued for decades, coming to an end only with the intelligence scandals of the 1970s.

Even such flagrant abuses as Operation Shamrock pale in comparison to the emergence of an information-age "surveillance-industrial complex." Nothing in our history compares to the efforts at mass surveillance now underway. Today's abuses combine the longstanding police impulse to utilize private-sector information sources with awesome new technological capabilities for vacuuming up, storing and keeping track of vast oceans of information. The ongoing revolution in communications, computers, databases, cameras and sensors, combined with the private sector's increasingly insatiable appetite for consumer information, have created new opportunities for security agencies. These agencies are increasingly relying on mass sorting, sifting, and monitoring of populations as a means of stopping terrorism.

---

[1] This report is available at: *http://www.aclu.org/national-security/combatting-surveillance-industrial-complex*.

[2] See Dana Priest and William Arkin, "A Hidden World, Growing Beyond Control," *Washington Post*, July 19, 2010.

Most of the interactions and transactions in Americans' lives are not conducted with the government, but with corporations and other private entities, who therefore hold most of the details of Americans' lives—including much of what is private and most important to them. From social networking to e-mail to photo sites, the more consumers learn, share, and connect online, the more personal information they leave behind. For example, as more people switch from hard-copy photographs in albums at home to online photo websites to develop and store digital photos, many do not realize that these photographs are stored in corporate databases, where they can be easily searched to compile information about consumers, their family and friends, and their private activities. As more people move information from hard copy calendars, address books, filing cabinets and home computers to online services, many do not realize that detailed information about who we know, where we go, and what we do in our personal lives could end up being collected and ultimately used in ways that we did not intend.

The combination of that rich detail with the awesome powers of the Federal Government is a prospect that ought to give every American pause, and that needs to figure prominently in evaluations of the privacy issues facing Americans today.

Security Agencies Have Many Options for Accessing Private-Sector Data

With the private sector tracking more and more of our activities for its own reasons, the government is free to leverage this private collection as a way of extending its own powers of surveillance.

Corporate compliance with government data-surveillance efforts ranges from unwilling resistance to indifferent cooperation to eager participation to actual lobbying of the government to increase such activities. With an array of options at its disposal, the government can acquire a valuable stream of information about private activities from any source. These techniques add up to a startling advance in government monitoring of American life.

The security agencies' options for accessing third-party information include:

Asking for data to be shared voluntarily. For example, in 2003, the online retailer eBay stated that it would be willing to give over all its information and everything it knows to law enforcement on request.[3] The C.I.A., via its investment arm In-Q-Tel, has invested in a software company that specializes in monitoring blogs and social networks.[4]

Buying information. Security agencies are not the only organizations that are interested in creating high-resolution pictures of individuals' activities by drawing together data from a variety of sources. Commercial data aggregators do the same thing for profit. These companies are largely invisible to the average person, but make up an enormous, multibillion-dollar industry. The Privacy Act of 1974 banned the government from maintaining information on citizens who are not the targets of investigations—but law enforcement agencies are increasingly circumventing that requirement by simply purchasing information that has been collected by data aggregators.[5] For example, the Department of Defense, the C.I.A., and the F.B.I. have all purchased use of private databases from Choicepoint, one of the largest aggregators of personal data.[6]

Demanding information, using legal powers granted by the Patriot Act and other laws. Section 215 of the Patriot Act gives the FBI the power to demand customer records from Internet Service Providers (ISPs) and other communications providers, libraries, book stores or any other business—with inadequate judicial oversight. National Security Letters, which can be issued by FBI officials in

---

[3] *http://lawmeme.research.yale.edu/modules.php?name=News&file=article&sid=925.* This policy seems to remain largely in force: according to eBay's current privacy policy, in response to a "verified request relating to a criminal investigation or alleged illegal activity," eBay will disclose "information relevant to the investigation, such as name, city, state, zip code, telephone number, e-mail address, User ID history, IP address, fraud complaints, and bidding and listing history."

[4] Noah Shactman, *U.S. Spies Buy Stake in Firm That Monitors Blogs, Tweets*, Wired, Oct. 19, 2009 at *http://www.wired.com/dangerroom/2009/10/exclusive-us-spies-buy-stake-in-twitter-blog-monitoring-firm/* (last visited October 23, 2009).

[5] See Chris Jay Hoofnagle, *"Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement," University of North Carolina Journal of International Law & Commercial Regulation*, Vol. 29 No. 4 (Summer 2004).

[6] Shane Harris, *FBI, Pentagon Pay For Access to Trove of Public Records*, NAT'L J., Nov. 11, 2005, available at *http://www.govexec.com/story page.cfm?articleid=32802* (last visited October 7, 2009); Robert O'Harrow Jr., *In Age of Security, Firm Mines Wealth Of Personal Data*, WASHINGTON POST at A01, Jan. 20, 2005, available at *http://www.washingtonpost.com/wp-dyn/articles/A22269–2005Jan19.html* (last visited October 7, 2009).

field offices without the approval of a judge, give the government broad power to demand records with no judicial oversight. In both cases, businesses can be subject to a gag order prohibiting them from talking about the government's data demands.

Using laws and regulations to dictate handling and storage of private-sector data in order to increase its surveillance value for the government. The Communications Assistance for Law Enforcement Act of 1994 (CALEA) forced telecommunications providers to design their equipment according to the FBI's specifications in order to make eavesdropping easier and more convenient. Another law mandates that airlines collect identifying information from their passengers so that the government, among other things, can keep records of who is flying where. And there are proposals for mandatory retention of communications data, which has been enacted in Europe and which the security establishment would like to enact in the United States.[7]

Creating systems for standing access to records of private activities. The Patriot Act expanded systems for the regular feeding of financial data to the government through "suspicious" transaction reporting,[8] and a system for the government to conduct broad-ranging, nationwide "Google searches" through financial records by giving the security agencies the power to order a search of financial institutions across the Nation for records matching a suspect.[9]

Other recent examples of close relationships between private-sector companies and government security agencies include:

The NSA spying scandal. When it was revealed that the NSA was conducting illegal warrantless eavesdropping within the United States, it quickly became apparent that several telecommunications companies were active and willing participants in this illegal and unconstitutional mass invasion of Americans' privacy. Congress eventually granted retroactive immunity to the companies despite the pending claims of those wholly innocent individuals whose privacy had been breached.

Fusion centers. Many proponents of these catch-all law enforcement data collection and analysis centers envision an active role for the private sector. Fusion Center guidelines crafted by the Department of Justice suggest the centers incorporate corporate participants, as well as private-sector data sources such as retail stores, apartment facilities, sporting facilities, hotels, supermarkets, restaurants, and financial companies.[10]

Solutions

There are at least two key areas for possible legislation or regulation which would not only protect consumer privacy but also limit the widespread collection of information by the government: data retention and third party access.

Data Retention

Currently, there is no uniform practice or industry standard regarding data retention limitations for information detailing consumers' online habits. The Federal Trade Commission has declined to regulate in the area of data retention, instead adopting a hands-off policy "[s]o long as self-regulation is making forward progress."[11] Other uses of online information likewise remain unregulated. The result has been disparate approaches to data retention among online industry leaders.

For example, Facebook collects a wide range of information about its users, including not only content created by the users themselves but also "[i]nformation we collect when you interact with Facebook". However, Facebook does not specify how long such information will be retained. Facebook also collects information when any

---

[7] See Declan McCullagh, "FBI director wants ISPs to track users," CNET News, Oct. 17, 2006; at *http://news.cnet.com/2100–7348 3–6126877.html*.

[8] The USA-Patriot Act, P.L. 107–56, Section 365, 115 Stat. 272 (Oct. 26, 2001). Scott Bernard Nelson, "Patriot Act would make watchdogs of firms," *Boston Globe*, November 18, 2001.

[9] "Financial Crimes Enforcement Network; Special Information Sharing Procedures to Deter Money Laundering and Terrorist Activity: Final Rule," 67 *Federal Register*, 60,579 (Sept. 26, 2002); the regulations stem from section 314 of the Patriot Act; Michael Isikoff, "Show Me the Money: Patriot Act helps the Feds in cases with no tie to terror," *Newsweek*, Dec. 1, 2003, online at *http://www.msnbc.com/news/997054.asp*.

[10] Bureau of Justice Assistance, Office Of Justice Programs, U.S. Dep't. Of Justice, "Fusion Center Guidelines: Developing And Sharing Information and Intelligence In A New Era," p. iii, (Aug. 2006).

[11] John Eggerton, *Liebowitz: FTC Not Interested In Regulating Behavioral Ads*, Multichannel News (May 12, 2010), available at *http://www.multichannel.com/article/452585-Liebowitz__FTC__Not__Interested__In__Regulating__Behavioral__Ads.php*.

logged-in user visits a third party website that contains a "like button" or "social plugin" the company's current policy allows it to retain this information for up to 90 days in identifiable format and to retain "aggregate and anonymized data" indefinitely.[12]

Search engine giants also have widely varying policies about data retention. Google retains a complete record of every search, including the user's complete IP address and cookie data if the user is logged into a Google account, for a full 9 months. It deletes part of the IP address after 9 months and deletes any associated cookie data after 18 months.[13] Microsoft retains complete search records for 6 months, deletes the entire IP address after 6 months, and deletes any associated cookie data after 18 months.[14] Yahoo! retains complete records for 3 months and deletes part of the IP address [15] as part of a "multi-step process to replace, truncate, or delete identifiers in order to de-identify data" after 3 months [16] before it completes an "anonymization," in which it deletes the last octect of the IP address. Google's cookie data used to track and analyze user search logs are retained for a full 18 months.[17]

These data retention limits are particularly important because they often apply to other services offered by the same company. Google, for example, offers not only a search function but also Gmail, Calendar, Maps, Picasa, YouTube, and various other services. Thus Google's data retention policy means that Google is able to retain and analyze data about users' web page visits, searches, online purchases, videos watched, posts on social networks, and other activities, for up to a year and a half. This creates an overwhelming, comprehensive, and intrusive picture of a user and his or her online behavior.

Imagine then if this vast amount of information were turned over to law enforcement or other government agencies. This would give the government unprecedented access to the lives and actions of law-abiding Americans and provide opportunities for government surveillance more intrusive than ever before. With access to the records held by online entities, the government could compile both broad and incredibly detailed profiles of people's activities and behaviors: not only who your friends are but where you met and how often you interact; not only which books you read but how you found them and which page you read most recently; not only which religion you claim but how often you actually attend services. The list of information that could be derived by government actors from data stored by private entities spans the entire spectrum of modern life.

Unfortunately, this "imaginary" scenario is all too real, as the line between commercial data and the government becomes increasingly indistinct. For example, in 2003 the online retailer eBay stated that "if you are law enforcement agency you can fax us on your letterhead to request information: who is that beyond the seller ID, who is beyond this user ID. We give you their name, their address, their e-mail address and we can give you their sales history without a subpoena." (sic) [18] Google reported that it received over 3,500 demands for information in the last 6 months of 2009.[19] If Google is receiving thousands of demands digging into the intimate de-

---

[12] Facebook Help Center, Social Plugins and Instant Personalization, *http://www.facebook.com/help/?faq=17512.* In addition, Facebook publicly announced this policy only after the press revealed the fact that the like button and social plugins allowed Facebook to collect this information. See Declan McCullagh, *Facebook "Like" Button Draws Privacy Scrutiny*, CNN.com, June 2, 2010, *http://www.cnn.com/2010/TECH/social.media/06/02/cnet.facebook.privacy.like/index.html.*

[13] See Google privacy FAQ at: *http://www.google.com/intl/en/privacy__faq.html#toc-anonymize.*

[14] See Bing Community, Updates to Bing Privacy, at *http://www.bing.com/toolbox/blogs/search/archive/2010/01/19/updates-to-bing-privacy.aspx.*

[15] *N.Y.Times,* Yahoo! Limits Retention of Personal Data, *http://www.nytimes.com/2008/12/18/technology/internet/18yahoo.html.*

[16] See Yahoo! Privacy Policy, Data Storage and Anonymization, at *http://info.yahoo.com/privacy/us/yahoo/datastorage/.*

[17] See Google privacy FAQ at: *http://www.google.com/intl/en/privacy faq.html#toc-anonymize.*

[18] See Lawmeme, Ebay to Law Enforcement, *http://lawmeme.research.yale.edu/modules.php?name=News&file=article&sid=925.* This policy seems to remain largely in force: according to eBay's current privacy policy, in response to a "verified request relating to a criminal investigation or alleged illegal activity," eBay will disclose "information relevant to the investigation, such as name, city, state, zip code, telephone number, e-mail address, User ID history, IP address, fraud complaints, and bidding and listing history."

[19] Government Requests Tool, *http://www.google.com/governmentrequests.* Note this does not include National Security letters or demands received outside of criminal investigations. It also does not count the actual number of users whose records disclosed pursuant to each demand. All of this means this number likely only reflects a fraction of the number of users whose records were demanded.

tails of individual lives captured in e-mails, search histories, reading and viewing logs, and elsewhere, how many more are going out to Yahoo, Microsoft, Facebook and the thousands of other online services that Americans use every day?

Reducing the amount of information held by private parties can address this threat without severely impacting Internet commerce. Recent research suggests that data reaches its maximum potential for marketing purposes in approximately twenty-four hours.[20] Forward-thinking companies have started to set data retention policies that reflect the reality that business needs do not require long retention times, while continuing to store data unnecessarily increases the privacy risks to consumers. Ask.com developed the AskEraser, allowing users to conduct online searches without the company logging any information. In 2008, Yahoo! announced an anonymization policy to de-identify most user log files records after 3 months. Yahoo!'s policy applies to user's web search data, information that tracks user's web page and advertisements views, and mouse click data.[21]

These consumer friendly policies demonstrate that it is possible to balance the need for innovative services and technological advances with the important priority of giving users adequate privacy protections. The ACLU encourages this committee to safeguard consumers by enacting mandatory data retention limitations for online service providers.

Third-Party Access

Online behavioral advertising and other online information services involve the collection of a staggering amount of information about people's online activities and the aggregation of that information in a few central locations.[22] For example behavioral marketers seek to form a thorough picture of users. They do so by combining information gleaned from different websites over time, including web page visits, searches, online purchases, videos watched, posts on social networking, and other sources.[23] Any particular website may provide little information, but when a large number of these data points are aggregated, the result is an extremely detailed picture.[24]

A striking recent development involves the potential to collect data from social networking sites like MySpace, Facebook, Twitter, and LinkedIn. Many of these sites explicitly allow third parties, including advertisers, to access information about their users through various means.[25] In addition, a scholarly paper reports that eleven of twelve sites studied had the potential to "leak" personally identifiable information about users unintentionally to advertisers and other third parties, including information such as name, address, phone number, gender, and birthday.[26]

The collection of this online information is frequently being matched with real-world, offline identities. One expert, Professor Ed Felton, recently discussed the

---

[20] See Jun Yan, Ning Liu, Gang Wang, Wen Zhang, Yun Jiang & Zheng Chen, *How Much Can Behavioral Targeting Help Online Advertising?* (2009),available at *http://www2009.eprints.org/27/1/p261.pdf*.

[21] *See* Yahoo.com, Yahoo! Privacy Policy: Data Storage and Anonymization, *http://info.yahoo.com/privacy/us/yahoo/datastorage/details.html* (last visited July 26, 2010).

[22] *Behavioral Advertising: Industry Practices and Consumers' Expectations: Hearing before the H. Subcomm. on Communications, Technology and the Internet of the H. Comm. on Energy and Commerce, and the H. Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 111th Cong. (2009) (Statement of Edward W. Felten, Professor of Computer Science and Public Affairs, Princeton University), available at *http://energycommerce.house.gov/Press 111/20090618/testimony—felten.pdf* (last visited October 7, 2009); id. (Statement of Jeff Chester, Executive Director, Center for Digital Democracy).

[23] Felten, *supra* note 15 , at 3–4; CENTER FOR DIGITAL DEMOCRACY, ET AL., ONLINE BEHAVIORAL TRACKING AND TARGETING: LEGISLATIVE PRIMER 2009 3, available at *http://www.uspirg.org/uploads/s6/9h/s69h7ytWnmbOJEV2uGd4w/Online-Privacy---Legislative-Primer.pdf* (last visited October 5, 2009); see also OMNITURE, THE RISE OF ONSITE BEHAVIORAL TARGETING 1 (May 2008) ("On-site Behavioral Targeting leverages each individual Web visitor's observed click-stream behavior, both on the current Web visit and from all previous visits, to decide what content is likely to be most effective to serve to that visitor."), available at *http://www.omniture.com/offer/281* (last visited October 7, 2009).

[24] Felten, *supra* note 15, at 3–4; Chester, *supra* n.15, at 8–10; Electronic Frontier Foundation, How Online Tracking Companies Know Most of What You Do Online (and What Social Networks Are Doing to Help Them), Sept. 21, 2009, *http://www.eff.org/deeplinks/2009/09/online-trackers-and-social-networks* (last visited October 7, 2009).

[25] These sites ordinarily provide some form of user control over this data sharing. However, approximately 90 percent of users do not take advantage of privacy controls to limit access by third parties. Chester, *supra* note 15, at 3. In addition, even when available and used, these controls often prove ineffective against technically-savvy snoopers. *Id.*

[26] BALACHANDER KRISHNAMURTHY & CRAIG E. WILLS, ON THE LEAKAGE OF PERSONALLY IDENTIFIABLE INFORMATION VIA ONLINE SOCIAL NETWORKS (2009) available at *http://conferences.sigcomm.org/sigcomm/2009/workshops/wosn/papers/p7.pdf* (last visited October 6, 2009).

process by which an online ad service might combine its user profile with information purchased from a commercial database: "If the ad service does know the identity, then third party services can provide a wealth of additional information, such as the user's demographics, family information, and credit history, which can be incorporated into the ad service's profile of the user, to improve ad targeting."[27] While Professor Felten was careful to make clear that "the fact that something is possible as a technical matter does not imply that reputable ad services actually do it,"[28] it seems likely the process is not uncommon. For example, the company Comscore, a leading provider of website analytic tools, boasts that "online behavioral data can . . . be combined with attitudinal research or linked with offline databases in order to diagnose cross-channel behavior and streamline the media planning process."[29]

This aggregated information can then be much more easily accessed by the government. This risk is certainly not theoretical. The FBI has admitted that it purchases information from "a lot of different commercial databases . . .," and stated that once that information is collected by those databases, "we legitimately have the authority to obtain 'that information'."[30] Given the government's demonstrated drive to access both online data and commercial databases of personal information, it seems nearly certain that law enforcement and other government actors will purchase or otherwise access the type of detailed profiles of online behavior compiled by behavioral marketers and others.

The best solution to this widespread surveillance of the American population is to limit the sharing of personal information with third parties and the aggregation of information into central databases. Limits on third party sharing would not hinder legitimate law enforcement investigations. Subpoenas and other law enforcement information gathering techniques would still be available to access records as part of an investigation. However, because personal information on innocent Americans would not be centralized, it would be harder to access and mass surveillance on the entire population would be more difficult. This is appropriate and necessary in our democracy. Innocent Americans have the right to be left alone. Detailed profiles of their interests, reading habits, and medical and financial information should not be readily available to their government.

Conclusion

As you consider the important issue of collection of personal information for business purposes, we hope that you will not lose sight of the government use of information collected online. As intrusive as this data collection and use of information may be when performed by individual online advertisers and service providers, it is even more alarming when this information is disclosed to the government. The current legal framework offers little meaningful protection against such surveillance. Therefore, it is crucial that new laws addressing online privacy create a framework for data retention limitations and bars on third party data collection that help limit unwarranted government access of this information.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN F. KERRY TO HON. JON LEIBOWITZ

Question 1. Chairman Leibowitz, in your roundtables and discussions at the FTC have you gotten a sense of the level of protection for privacy consumers believe exists in the law for the information they share online and how that compares to the actual protections in law?

Answer. A number of the stakeholders that participated in the FTC's privacy roundtables discussed consumers' interest in the privacy of their personal information. For example, roundtable participants cited a study showing that consumers were willing to pay more to shop at websites that have better privacy policies, as well as other consumer surveys that consistently indicate that a majority of consumers are uncomfortable with being tracked online.

Despite this concern, it appears that consumers, in large, do not understand the extent to which their data is collected online or how that data is used and shared with third parties. Some of this confusion is the result of the invisibility of many online data practices. In addition, it appears that consumers often believe that there are laws that prevent certain data practices. Survey evidence provided during our roundtable project showed that consumers have very little understanding regarding

---

[27] Felten, *supra* n.15 at 4.

[28] *Id.*

[29] Why Comscore?, *http://comscore.com/About_comScore/Why_comScore* (last visited October 6, 2009). 30Harris, *supra* n.5 (quoting F.B.I. spokesman Ed Cogswell).

[30] Harris, *supra* n.5 (quoting F.B.I. spokesman Ed Cogswell).

the laws that govern how companies may collect and use data. Many consumers believe, for example, that if a company has a privacy policy, the company is not permitted to share a consumer's information with other companies without the consumer's permission. Accordingly, there appears to be a gap between what many consumers expect about the information they share online and what many companies are, in fact, doing with such information. Educating consumers about data practices—both online and offline—remains a challenge, especially in light of rapidly changing technology and the development of new business models.

Question 2. Chairman Leibowitz, do you believe that the private sector is meeting existing consumer expectations of privacy and is there something different about firms operating on the Internet versus firms that operate offline in terms of how much information they are collecting or the principles that should govern their operations?

Answer. Although, as noted above, there appears to be a gap between some consumers' privacy expectations and actual practices, we have seen steps by industry to improve the transparency of their data practices and to offer consumers better tools to control the collection and use of their data. For instance, since the FTC issued its online behavioral advertising principles in 2007, a number of individual companies have developed new disclosures and tools to allow consumers to control their receipt of targeted advertisements. These are positive steps; however, we believe that industry needs to continue to improve its data practices in order to meet consumers' privacy expectations. This is true regardless of whether companies are collecting consumer data online or offline. Indeed, more companies appear to be merging data collected online and offline, rendering the distinction between the sources of collected data less meaningful.

Question 3. Chairman Leibowitz, there are some who argue that the reason Google, Facebook, Yahoo and others are American firms and not European firms is due in part to their freedom to collect and use information here versus that allowed in Europe. Chairman Leibowitz, could you talk about privacy standards in Europe and how they compare to those here as well as what effect the disparity in rules has had on opportunities for innovation?

Answer. Although the United States and Europe have different regulatory frameworks in the area of online privacy, we share the same goals. Specifically, we both want transparency, and for consumers to have control over who obtains their data and what is done with it. In addition, we each want reasonable security for personal information and expect and demand accountability from businesses that handle consumer information. Although there are already many harmonized goals, the difference lies in how they are achieved. A number of different factors, like enforcement priorities, the role of self-regulation, and freedom of expression, are implicated in how privacy is approached. Given these factors, a completely harmonized approach between the U.S. and Europe is challenging.

The FTC has received feedback from U.S. industry that transborder data flows are a particular challenge in the privacy area, particularly when it comes to compliance costs and confusion as to how to even comply with laws in different jurisdictions. I do think that the requirement in European law that transfers of personal data outside of Europe can only occur when the receiving countries have been determined to have "adequate" protections has created certain compliance challenges. U.S. companies are looking for streamlined ways to meet those challenges, such as the U.S.-EU Safe Harbor Framework for data transfers, so that they can continue to innovate and develop new products for consumers.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN F. KERRY TO GUY "BUD" TRIBBLE

Question 1. Mr. Tribble, technically, can firms at the browser level (Chrome, IE, Safari, etc.) establish private browsing capacity that would allow users to establish a baseline standard of protection that every site they visit would have to acknowledge and respect?

Answer. Today, when using a browser to surf the Internet, individuals have a number of built-in browser features to help reduce the amount of unintended information shared directly with any particular website or stored on one's own computer. A considerable amount of the unintended information exchanged with visited websites and often used to monitor a user's interactions with those websites comes directly from browser cookies. While the Apple Safari browser, for example, is already configured by default not to allow third-party website cookies from being placed on one's computer, an individual also can turn off browser cookies entirely. However, turning off cookies from the browser will not prevent some third-party

plug-ins or extensions, installed by the user, from placing their own cookies and exchanging information with websites. Those cookies must be managed separately by the plug-in. But there are also trade-offs as turning off cookies may degrade or disable many useful features on any given website. For example, on some websites a shopping cart may no longer store items or function at all.

Managing cookies or turning them off entirely at the browser level is not enough to establish complete user privacy while surfing online. Modern browsers have evolved by giving users greater control over cookies and other mechanisms that websites might use to store information on the user's local computer—information which can be used to identify that browser while surfing. However, even with these privacy features, browsers cannot prevent websites from recognizing unique characteristics of the browser, the operating system and the network being used, and thus websites remain able to register information about the user's browsing. In order to connect with the user's browser and properly present web pages, websites are inherently able to identify such unique characteristics as a user's IP address, the type of browser being used and its version, the operating system and its version, its language, the plug-ins installed, installed fonts, and the screen resolution, among others. Taken together, these characteristics present enough information and are often variable enough to establish a unique profile for every website visitor. Once visited, a website would be able to identify a visitor each time he/she came back even with cookies turned off and private browsing enabled. Completely preventing this kind of information from flowing from the browser to the website during normal operation is an unsolved (and very difficult) technical issue. It may not even be possible to do while maintaining the efficiency and usability of the Web. It is for these reasons that we do not believe that browser level management alone can establish a complete baseline private browsing capacity that every website would have to acknowledge and respect.

Question 2. Mr. Tribble, Apple teams with AT&T for the delivery of services to the iPhone and iPad. How are responsibilities for privacy protection distributed between your two companies?

Answer. Apple is strongly committed to protecting the privacy of its customers. As we state in our Privacy Policy, we collect and share only the information that is necessary for AT&T to complete its activation process and to carry out its service. Once the data is given to AT&T, the data in their possession is treated in accordance with their privacy policy including their security practices. Data retained by Apple is governed by our privacy policy. As we stated in our testimony, Apple does not share the personally identifiable information of its customers with third parties for their marketing purposes.

Question 3. Mr. Tribble, does Apple support baseline privacy protections in legislation and do you support either of the pending bills in the House and if not, what exactly would baseline protections include?

Answer. Apple supports baseline privacy protections governing clear notice and choice over the use of information, particularly personally identifiable information. As we have described in detail in our testimony, Apple is strongly committed to protecting the privacy of its customers by giving them control over the collection and use of their personal information and their location, and we believe that our products do this in a simple, elegant and transparent way. Further, as we stated in our testimony, Apple does not share the personally identifiable information of its customers with third parties for their marketing purposes. Finally, with respect to the legislative proposals and discussion drafts circulating on Capitol Hill to address online privacy, Apple has been working closely with our U.S. based technology industry colleagues and through our trade associations on matters governing consumer online privacy protections.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN D. ROCKEFELLER IV TO BRET TAYLOR

Question1. Are Facebook users given the ability to review and approve what posts, videos, or photos of them are being "tagged" or labeled before they are posted publicly by others?

Answer. Facebook offers users controls that enable them to determine what they share and with whom they share it. Facebook's system also offers users the ability to control who has permission to post on their Wall or comment on the content they share. Only people who have been confirmed by a user as friends can tag that user in third-party content, and users can control who has permission to see an aggregated view of content in which they have been tagged. For example, Last year Facebook introduced "per-object-privacy control," an unprecedented tool, which al-

lows users to determine on an item-by-item basis how broadly they want to share particular content. Similarly, this year, Facebook deployed an innovative setting that gives users a simple, one-click control over how widely they share their information. Facebook also provides users the ability to determine, when they are identified in content shared by other users, whether and the extent to which that identification is shared with other Facebook users. Users are also notified when they are tagged and can remove those tags so that they are no longer associated with that content. Finally, Facebook users have a setting they can use to determine whether and the extent to which photos and videos in which they are tagged are visible to other users.

Facebook also sets forth rules in our Statement of Rights and Responsibilities ("SRR") that make clear the types of content and behaviors that are prohibited on the site. The Facebook community of more than 500 million users takes the requirements in this SRR seriously. On the occasion when some users share content that other users feel violates our SRR, the community of users clicks our ubiquitous "Report" links, found throughout the site. This sends a report to Facebook's User Operations team that reviews reported content every hour of every day. Where we determine that content is in violation of the SRR, it is removed. When a user's behavior is particularly inappropriate or when action has been taken regarding that user's account on more than one occasion, that user's account may be disabled. In short, our users act as community police who enforce the standards of decency embodied in our SRR. This innovation has helped Facebook grow dramatically while keeping Facebook relatively free of inappropriate or offensive content.

Finally, in the event that users post illegal content, we take appropriate action as soon as we are made aware of that content. We work closely with law enforcement at the Federal, state, local and international level. We have developed a strong partnership with the National Center for Missing and Exploited Children ("NCMEC"). In addition to developing methods of blocking the distribution of images of child sexual exploitation or violence that we encounter, we share unlawful images we encounter with either NCMEC or law enforcement as appropriate.

Question 2. If not, has there been any consideration to give users this type of control?

Answer. Facebook continually assesses and seeks to improve its privacy and sharing controls. We believe that our current framework—which combines industry-leading sharing controls, coupled with robust community-based enforcement—provides users the best possible experience. Facebook's community of users plays an important role in determining what information is posted, when and with whom it is shared. They also play a critical role in helping to keep Facebook free of inappropriate content. The innovative approach Facebook employs of "crowd sourcing" the identification and reporting of potentially inappropriate content on the site has allowed Facebook to grow without becoming an unpleasant place to visit. This practice motivates users to police the site and deters inappropriate conduct and content.

Question 3. How straightforward and conspicuous is it for a Facebook user to permanently delete an account?

Answer. Account deletion on Facebook is straightforward. Facebook users who want to delete their account may do so by clicking on the drop down menu under Account, found at the top of each page, and navigating to the Help Center. Currently, the first topic mentioned under "Common Searches" is "delete account," with a hyperlink to the appropriate "Frequently Asked Question" page. The answer to the question "how do I delete my account?" includes a hypertext link to an explanation and a button the user can click to initiate account deletion.

Question 4. What is the process?

Answer. Please see the response to Question 1 immediately above.

Question 5. Have there been complaints about the deletion process?

Answer. In addition to user inquiries, in 2009 the Office of the Privacy Commissioner of Canada ("OPC") responded to a complaint raised by the Canadian Internet Policy and Public Interest Clinic alleging that Facebook made account deletion cumbersome. As a result, Facebook, in conjunction with the OPC, agreed to modify the descriptions of deactivation and deletion on Facebook and to make access to both processes more prominent.

Question 6. Does a deleted account imply that all your information is erased?

Answer. When a user deletes an account, the account is permanently deleted and cannot be reactivated by the user. However, as noted in our Statement of Rights and Responsibilities, "removed content may persist in backup copies for a reasonable period of time." In addition, as explained in our Privacy Policy, "[e]ven after you remove information from your profile or delete your account, copies of that in-

formation may remain viewable elsewhere" based on the distributed nature of shared content.

Question 7. If not, do Facebook users understand this?

Answer. As a condition of using the Facebook site our users agree to abide by the Statement of Rights and Responsibilities. Users are responsible for reading and understanding the terms of the Statement of Rights and Responsibilities including the provisions that discuss Facebook's deletion policy. Facebook also provides prominent links to, and encourages users to review, its Privacy Policy, which as noted above includes information regarding account deletion.

Question 8. Where and how is a user's information retained and for what purposes?

Answer. Facebook user information is stored on a network of servers located in the United States. We store information in this manner so that we may provide Facebook to our users and allow each user to obtain access to information they have shared or that was shared with them through Facebook.

Question 9. Can an account stay deactivated indefinitely?

Answer. Yes. On occasion, some Facebook users want a way to step away from Facebook for a period of time without deleting the account. Users who deactivate do so for many reasons, including that they are busy with school or preparing for exams, are on a vacation or sabbatical, become ill, or are traveling for work. We make clear to users who deactivate their accounts that they may reactivate at any point in the future, and the vast majority of users who deactivate eventually do so.

Question 10. If not, after what amount of time does a deactivated account permanently delete?

Answer. Please see the answer to (1) immediately above this section.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN F. KERRY TO BRET TAYLOR

Question 1. Mr. Taylor, there is some question about how long service providers should hold a person's information. When a user deactivates his account, but does not delete it, how long do you keep the information and why?

Answer. Our experience suggests that occasionally some of our users want a way to step away from Facebook for a period of time but do not wish to eliminate the accounts they've created. For such users, we offer account deactivation. Although a deactivated account is inaccessible to other Facebook users, we retain that account indefinitely. Users who deactivate do so for many reasons, including that they are busy with school or preparing for exams, on a vacation or sabbatical, become ill, or traveling for work. We make clear to users who deactivate their accounts that they may reactivate at any point in the future, and the vast majority of users who deactivate eventually do so.

Question 2. Mr. Taylor, does Facebook support baseline privacy protections in legislation and do you support either of the pending bills in the House and if not, what exactly would baseline protections include?

Answer. We support enactment of baseline privacy protections such as those that enhance disclosure, increase transparency, and provide users with control over data, but that also still permit innovation.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN F. KERRY TO DR. ALMA WHITTEN

Question 1. Ms. Whitten, Google has made it clear that the collection of information from WiFi networks was a mistake and promises not to do it again. First, as the Chief Privacy Officer are Google practices not reviewed by your office and how was this missed? Second, if it was a mistake and not illegal, couldn't others right now be using similar techniques to steal information from WiFi networks?

Answer. Thank you. As you note, Senator Kerry, this was an error for which we are profoundly sorry, and we are determined to learn all the lessons we can from our mistake.

We are still reviewing our processes and the facts in this instance to understand how and why this occurred, but I can say as Google's Privacy Engineering Lead that it was not consistent with the value we place on the responsible collection of data. Google is taking the review of this matter very seriously and we will report back with the changes we'll make to prevent such a thing from happening in the future.

We appreciate your concerns about the potential misuse of WiFi technology. In fact, Google offers encrypted e-mail and search to help protect our users from others who might misuse their data. We remain the only major online provider to encrypt our e-mail service by default.

We also urge WiFi users to activate encryption settings on their WiFi routers. While some may prefer to leave their WiFi signals configured so as to be readily available to the general public, we believe most users would be best served by encrypting their communications—which would offer them both technological and legal protection.

Question 2. Ms. Whitten, technically, can firms at the browser level (Chrome, IE, Safari, etc.) establish private browsing capacity that would allow users to establish a baseline standard of protection that every site they visit would have to acknowledge and respect?

Answer. This is an important idea to pursue, Senator. Our product and engineering teams work hard to offer industry-leading privacy tools to users of all of our products, including Google Chrome.

Browser-based efforts to enforce website privacy practices have unfortunately failed in the past. Website operators are not under the control of the browser providers, and so the browser cannot evaluate the practices of any website beyond its representations. The *Platform for Privacy Preferences Project*, or P3P, sought to implement a solution along these lines a decade ago, but was unable to overcome major implementation and enforcement hurdles.

Nevertheless, we continue to work with technical groups and internally on developing robust browser privacy controls. While browsers cannot perfectly enforce what happens with data at the other end of the Internet connection, responsible providers should respect the preferences that the user indicates through browser settings.

Chrome of course already offers Incognito Mode, in which webpages that a user opens and files downloaded are not recorded in the user's browsing and download histories. In addition, all cookies set in Incognito Mode are deleted after a user closes browser windows that she has opened. These features would prevent persistent cookies and other tracking mechanisms, if a user prefers a less personalized web experience.

Note also that the use of cookies for personalization, targeted advertising, and analytics remains always under the control of the user. Moreover, they can recognize a browser on an anonymous basis without requiring a user to log in and reveal his or her identity. As Princeton University computer scientist Ed Felton *wrote*, "if a site is going to track me, I want them to do it openly, using cookies." Google goes even further, by offering industry-leading opt-out mechanisms.

Question 3. Ms. Whitten, does Google support baseline privacy protections in legislation and do you support either of the pending bills in the House and if not, what exactly would baseline protections include?

Answer. Yes, Google supports the development of comprehensive, baseline privacy legislation that can ensure broad-based user trust, support continued innovation, and serve the privacy interests of consumers. As I wrote in my testimony, I believe such legislation should at the least include:

- *Even-handed application* to all personal data regardless of source or means of collection.
- *Recognition of benefits and costs* of legislating in this area, including explicit attention to actual harm, compliance costs, and continued online innovation.
- *Uniform, reasonable security principles*, including data breach notification procedures.
- *Clear process for compelled access*. The U.S. law governing government access to stored communications is outdated and out of step with what is reasonably expected by those who use cloud computing services.
- *Consistency across jurisdictions*. Generally, Internet users neither expect nor want different baseline privacy rules based on the local jurisdiction in which they or the provider reside.

At Google, we believe that stable, baseline principles set by law can permit flexible, adaptive self-regulatory structures to develop on top—much like the stable protocols and standards at the physical and network layers of the Internet allow flexible and innovative development at the content and application layers.

We would be glad to work with you and your staff on this important matter, as we share the same goal of increasing trust and security for all Internet users.

We are encouraged by the sincere effort toward this goal represented by the House bills to which you refer in your question. We have provided direct feedback

to Chairman Boucher on his draft, a copy of which we have attached to these responses. We are still reviewing the bill introduced by Chairman Rush, and we look forward to working with his office on this issue as well.

Thank you again for the opportunity to address the Committee.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN F. KERRY TO PROFESSOR JOSEPH TUROW

Question 1. Professor Turow, you have done research indicating that most consumers do not want firms using their information to target ads to them. Yet industry argues that once they explain to users that they receive ads more likely to be of interest to them this way, the concern disappears. How do you respond to the industry argument that most people benefit from the collection and use of their information and most are not concerned once educated?

Answer. The research I carried out with colleagues at the University of California, Berkeley, Law School showed that a majority (66 percent) of Americans do not want ads "tailored to your interests." The percentage gets much higher when the people who said they want tailored ads were told that that firms follow their activities in various ways (on the website they are visiting, on other websites they have visited, and in stores) in order to present the tailored material to them. Then many of those people as well tend to say they didn't want they ads, with percentages varying dependent on where they would be followed. In the end, around 80 percent of Americans said they didn't want the tailored advertising.[1]

Two points ought to be emphasized about this research.

- First, the research was conducted in a "gold-standard" manner. The well-known firm Princeton Research interviewed 1,000 randomly chosen Americans via both landline and cell phones according to the best academic criteria for carrying out this work. Although interviewing people by phone—and especially on cell phones—is expensive, it is far preferable to using the Internet to recruit and interview individuals. Many, if not most, industry surveys use people recruited via the internet. These cannot be random by their very nature because the people volunteer in response *to ads they see*. Moreover, there is the real danger that people who volunteer over the Internet feel more comfortable doing things online than the population as a whole. Consequently, their answers to questions about their knowledge about the Internet and comfort with it cannot be seen as reflecting the views of the population as a whole.
- Second, the findings of our study about tailored advertising are very much in line with findings of previous national telephone surveys I have conducted. Moreover, our tailored-advertising study showed that Americans' concerns about being followed are not just focused on advertising. We asked questions about tailored discount coupons as well as tailored news. The percentages were different; 57 percent didn't want tailored news while 49 percent didn't want tailored advertising. But when people who said tailored discount coupons and news are OK were told that they were being followed in order to get the information used for that customization, many of those people said they didn't want it. That brought the percentages of Americans saying no to tailored discounts and news around 80 percent. We conclude, then, that Americans don't say no to tailored advertising because they dislike advertising and find it annoying. They say no, as they say no to tailored discounts and news, because they dislike the idea of firms following them around online and offline.

A number of organizations representing Internet marketers have conducted research to try to rebut our findings. Their studies were done using Internet samples that are not representative. Yet they still confirm our result that in huge numbers Americans say they do not want tailored advertising. Using an online survey where at least 50 percent were recruited online, Datran tried a somewhat different tack to argue that most Americans "are not concerned once educated." First Datran asked similar questions about advertising to the ones our studied asked, and it found similar results. Then the people were told about the following information called PreferenceCentral and then asked the question (Q9) below it:[2]

---

[1] Joseph Turow, Jennifer Kind, Chris Jay Hoofnagle, Amy Bleakley and Michael Hennessy, "Americans Reject Target Advertising," Annenberg School for Communication & Berkeley Law School, September 2009. Electronic copy available at: *http://ssrn.com/abstract=1478214*.

[2] Datran, "Preference Central: Consumer Perspectives on Online Advertising 2010," Datran Media Powerpoint Slide Presentation, July 2010.

PreferenceCentral is a free service that provides consumers with complete control of what targeted advertising they receive online and complete visibility into what information advertisers use to target the advertisements. More specifically, *PreferenceCentral* provides consumers:

Complete Control: Consumers will now be able to select what online advertising they will get—Selecting the categories, brands, or advertisers they are interested AND those they do not want;

Complete Transparency: Consumers will now know what information is being used by specific advertisers to target advertising to them AND have that specific advertiser stop use of that information for targeting. This will happen through a notification in every targeted ad that links to an account where a consumer can exercise control;

Monitoring and Enforcement: PreferenceCentral will also monitor online advertising to assure that consumers' preferences and industry best practices are being used by advertisers.

Q9. Based on this description of *PreferenceCentral*, how interested would you be in using this free service?

Extremely Interested (5)
Very Interested (4)
Somewhat Interested (3)
Not Very Interested (2)
Not At All Interested (1)

Datran says that after hearing the description about PreferenceCentral, "41 percent became more comfortable." (It seems, though, that a substantial segment was still uncomfortable.) The company therefore posits that once educated and assured about protections, most Americans will be OK with tailored advertising. The problem is that the PreferenceCentral service that they describe for their subjects simply doesn't exist. Moreover, this kind of universal "complete control" and "complete visibility into what information advertisers use to target" is not a serious possibility at this time. As a result, people are responding to an unrealistic hypothetical that gives them assurances that won't be achieved. For all intents and purposes, then, the findings agree that in the contemporary situation it will be difficult to sway Americans from being uncomfortable with tailored advertising. To simply say that Americans' concerns disappear "when they are educated" is disingenuous.

Furthermore, PreferenceCentral and other self-regulatory programs obscure the underlying issue: these programs still allow advertisers to track users pervasively. The "control" mechanism speaks to what ads the individual will receive, not to whether they can reject tracking. Much of our survey concerns the underlying data practices that advertisers are unwilling to address. For instance, we found that Americans strongly favor laws giving them a right to delete, a right to transparency, a right to vindicate wrongs in court for money damages, and for a requirement that advertising companies delete data after a certain amount of time. The industry's surveys and self-regulatory programs do not address any of these issues.

As for the industry's argument that most people benefit from the collection and use of their information, the industry has not shown that most people believe that based on the ways that marketers and media firms are collecting and using their data. Apart from survey research that I have conducted, alone and with colleagues, other surveys and many qualitative studies and anecdotal reports suggest that people do not buy the cost-benefit calculation that the industry insists they accept.

Question 2. Professor Turow, if there were a single stand out private sector actor that is doing right by consumers on privacy, who would you cite?

Answer. It's difficult to cite such a company, especially among the major players. The key point to be made is the competition in the contemporary media scene is virtually forcing companies to ratchet up their ability to track people and exchange increasingly deep and "social" information about them. There is no market for digital privacy, partly because consumers do not have an opportunity to make selections based on privacy criteria.

Question 3. Professor Turow, do you support either of the pending bills in the House and if not, what exactly would baseline protections include?

Answer. I would prefer to state baseline protections. They include the following:

(1) *A universal opt-in "do not follow" mechanism should be established for consumers across the digital space*. Consumers could adopt some universal mechanism, such as a "DONOTTRACKME" setting in their http headers, that would signal to website that the user does not want to be tracked. Having this tag

would mean that advertisers could not track that person's computer and that sites the person visits could not offer the person's data on an exchange. It *would* allow individual sites to follow people around those sites and send targeted commercials based on those activities. This plan would not require a lot of work on the part of many parties to construct and implement, because the infrastructure of the NAI opt out is already in place. Advertisers would simply have to look for the DONOTTRACKME setting, rather than an opt out cookie, which are easily deleted.

(2) *With every targeted commercial message, a link should lead to the presentation of the following information*:

a. Names and links to the companies involved in the targeting

b. Descriptions of the specific data they collected and where they got the data

c. How the targeting took place—for example, as a result of cookies or registration or Flash Cookies; sold by the site, through an exchange; or via an ad network

d. How to change some of the data, opt out of certain data use by those firms, or fully opt out of the site and/or the marketers following the consumer

(3) Enhancement of data should be prohibited unless the person gives explicit permission. Advertisers have long argued that consumers could control their privacy by limiting revelation of personal information. This is good advice, but can be completely undone through the practice of "enhancement." Enhancement is a process where advertisers "overlay" or "bump up" customer databases by adding information from other sources. It adds to the data points organizations have to use about citizens in ways that are beyond the citizens' control or knowledge. Enhancement takes place when a party with certain information about a person gets more information about that person from another provider of the data. That may happen through anonymous cookie matching. It may take place when a publisher or marketer uses personally identifiable registration data from its visitors to buy more information about them from data firms. It may also happen when a publisher, marketer, or data firm gets anonymous individuals to identify themselves (by signing up for sweepstakes, for example) and then purchases information about the person from various sources. In some of these cases, the organizations may re-anonymous the individuals.

○