NEW TECHNOLOGIES AND INNOVATIONS IN THE MOBILE AND ONLINE SPACE, AND THE IMPLICATIONS FOR PUBLIC POLICY

HEARING

BEFORE THE

SUBCOMMITTEE ON
INTELLECTUAL PROPERTY,
COMPETITION, AND THE INTERNET

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

JUNE 19, 2012

Serial No. 112–116

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE

74–641 PDF WASHINGTON : 2012

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

COMMITTEE ON THE JUDICIARY

LAMAR SMITH, Texas, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
STEVE CHABOT, Ohio
DARRELL E. ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
DENNIS ROSS, Florida
SANDY ADAMS, Florida
BEN QUAYLE, Arizona
MARK AMODEI, Nevada

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
MIKE QUIGLEY, Illinois
JUDY CHU, California
TED DEUTCH, Florida
LINDA T. SÁNCHEZ, California
JARED POLIS, Colorado

RICHARD HERTLING, *Staff Director and Chief Counsel*
PERRY APELBAUM, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON INTELLECTUAL PROPERTY, COMPETITION, AND THE INTERNET

BOB GOODLATTE, Virginia, *Chairman*
BEN QUAYLE, Arizona, *Vice-Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
STEVE CHABOT, Ohio
DARRELL E. ISSA, California
MIKE PENCE, Indiana
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
SANDY ADAMS, Florida
MARK AMODEI, Nevada

MELVIN L. WATT, North Carolina
JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
JUDY CHU, California
TED DEUTCH, Florida
LINDA T. SÁNCHEZ, California
JERROLD NADLER, New York
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
HENRY C. "HANK" JOHNSON, JR., Georgia

BLAINE MERRITT, *Chief Counsel*
STEPHANIE MOORE, *Minority Counsel*

CONTENTS

JUNE 19, 2012

Page

OPENING STATEMENTS

The Honorable Bob Goodlatte, a Representative in Congress from the State of Virginia, and Chairman, Subcommittee on Intellectual Property, Competition, and the Internet 1

The Honorable Melvin L. Watt, a Representative in Congress from the State of North Carolina, and Ranking Member, Subcommittee on Intellectual Property, Competition, and the Internet 2

The Honorable Lamar Smith, a Representative in Congress from the State of Texas, and Chairman, Committee on the Judiciary 4

The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Ranking Member, Committee on the Judiciary, and Member, Subcommittee on Intellectual Property, Competition, and the Internet 5

WITNESSES

Scott R. Shipman, Associate General Counsel, Global Privacy Leader, eBay Inc.
Oral Testimony 8
Prepared Statement 10

Morgan Reed, Executive Director, Association for Competitive Technology
Oral Testimony 19
Prepared Statement 22

Chris Babel, Chief Executive Officer, TRUSTe
Oral Testimony 33
Prepared Statement 35

James Grimmelmann, Associate Professor of Law, New York Law School
Oral Testimony 62
Prepared Statement 65

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Response to Post-Hearing Questions from Scott R. Shipman, Associate General Counsel, Global Privacy Leader, eBay Inc. 98

Response to Post-Hearing Questions from Chris Babel, Chief Executive Officer, TRUSTe 100

Response to Post-Hearing Questions from James Grimmelmann, Associate Professor of Law, New York Law School 103

Prepared Statement of the Consumer Electronics Association (CEA) 104

OFFICIAL HEARING RECORD

MATERIAL SUBMITTED FOR THE HEARING RECORD BUT NOT REPRINTED

February 2012 White House green paper entitled Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. This paper is on file at the Subcommittee and can be accessed at: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

March 2012 FTC report entitled Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers. This report is on file at the Subcommittee and can be accessed at: http://www.ftc.gov/os/2012/03/120326privacyreport.pdf

March 2012 report, a project of the Pew Research Center, entitled Search Engine Use 2012. This report is on file at the Subcommittee and can be accessed at: http://pewinternet.org/~/media//Files/Reports/2012/PIP__Search__Engine__Use__2012.pdf

NEW TECHNOLOGIES AND INNOVATIONS IN THE MOBILE AND ONLINE SPACE, AND THE IMPLICATIONS FOR PUBLIC POLICY

TUESDAY, JUNE 19, 2012

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INTELLECTUAL PROPERTY,
COMPETITION, AND THE INTERNET,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to call, at 10:07 a.m., in room 2141, Rayburn House Office Building, the Honorable Bob Goodlatte (Chairman of the Subcommittee) presiding.

Present: Representatives Goodlatte, Smith, Chabot, Poe, Chaffetz, Marino, Watt, Conyers, Chu, Deutch, Lofgren, Jackson Lee, and Johnson.

Staff Present: (Majority) Vishal Amin, Counsel; Olivia Lee, Clerk; and (Minority) Stephanie Moore, Subcommittee Chief Counsel.

Mr. GOODLATTE. Good morning. This hearing of the Subcommittee on Intellectual Property, Competition, and the Internet will come to order, and I will recognize myself for an opening statement.

Today we are holding a hearing to examine the public policy issues raised by new technologies in the mobile and online spaces. It is clear that some of the central policy issues for both consumers and companies are the issues of privacy and data collection. Privacy continues to take on greater importance as more Americans not only use the Internet and mobile devices, but also share their personal information with companies on the Web. Privacy policies and the technological safeguards that companies implement will help guide consumers on what they should expect from those who handle their personal information and set expectations for companies that use personal data.

As Congress continues to look at privacy issues online, it is important to have a firm understanding of what the industry practices are. Today's hearing will explore what mechanisms the private sector is currently employing to protect Internet and mobile users. It will also highlight the technological innovation and development that has occurred in this space.

There have been astonishing advancements in the delivery of products and services online, and as a result there are privacy implications for a variety of new technologies, some of which were not even in existence a few years ago. Many in the private sector al-

ready have policies and procedures in place to police themselves to ensure they are following best practices. Groups like TRUSTe, the Association for Competitive Technology, the Application Developers Alliance, the advertising industry through its AdChoices program and others already help to provide best practices, independent analyses of privacy policies, and recommendations for enhancements. We will learn more about how some of these groups work in the field today.

As Congress begins to look into these issues, we need to realize that the technologies that we are discussing did not even exist a few years ago, and some have only come to the forefront in the past few months. And with any new technology, it is important that as we think about how best to protect the interests of consumers and the Internet user community, we continue to encourage and not stifle innovation.

One of the most important things private-sector companies can do to self-regulate and innovate when it comes to privacy is to make their notices and privacy policies easy to understand. If the consumer understands the trade-off he makes when he accepts an app program or service, then the consumer will make an informed decision.

The easier it is for consumers to understand all privacy notices and policies, the easier it is for companies to compete on the basis of their privacy policies, and the easier it is for consumers to vote with their wallets.

I look forward to hearing from all of our witnesses on the efforts that they have taken to help build in privacy protections. As they develop their products to safeguard consumer information about what more can be done to increase transparency and ensure that as American companies seek to operate abroad in markets like Europe and Asia, innovation is not impeded by undue regulatory burdens or barriers to market access.

And with that it is my pleasure to recognize the Ranking Member of the Subcommittee, the gentleman from North Carolina, Mr. Watt.

Mr. WATT. Thank you, Mr. Chairman. I appreciate you holding this hearing.

I believe that privacy is one of the most fundamental values of the American tradition, yet today even a majority of the Justices of the Supreme Court posit that as a society we are faced with novel challenges in determining the, quote, "new normal," close quote, for privacy expectations in the digital age.

There is little doubt that the digital environment has created opportunities for society that often come at little or no financial cost to the user, but I believe it is inappropriate to classify these opportunities and services as free. Information is currency, and users are, without exception, required to surrender incredible amounts of personal information in exchange for the services they enjoy.

While Internet users have some responsibility to self-censor and restrict the intimate information they share on various platforms, the reality is that many online users have a false sense of privacy because they don't understand the lengthy and complex privacy policies they are compelled to agree to in order to use the service.

As a result, online users often share lots of personal information unknowingly and to unintended audiences.

Their personal information has been marshaled, analyzed and monetized in ways consumers have come to resent. A March 2012 study by the Pew Research Center found that two-thirds of Internet users have negative views about search engines collecting information about them to produce personalized search results. Two-thirds of Internet users also report that they, quote, "are not okay with targeted advertising because they do not like having their online behavior tracked and analyzed."

I am further concerned that this type of consumer profiling may limit, rather than enhance, the experience and the horizons of distinct groups based on race, ethnicity, religion and other factors that we are probably not even aware of yet. If users are constantly fed products and facts in areas in which they or someone like them have already expressed an interest, their intellectual curiosity and development may be stunted.

Earlier this year both the Department of Commerce and the Federal Trade Commission completed reports following stakeholder participation to address mounting concern about consumer privacy. The White House Green Paper enumerated seven broad principles that it urges be enacted into law as flexible baseline standards governing consumer privacy.

The Green Paper recommends that industry leaders develop specific codes of conduct to implement for consumer privacy principles. The FTC's report takes the additional step of identifying best practices that could, and I believe should, serve as a guide for industry in developing the codes of conduct.

The Administration has determined that the first round of stakeholder meetings will center on mobile applications which raise serious questions about the security of data concerning children and geolocation information concerning all users. Parents must be able to feel secure that the apps they download to educate or entertain their children aren't secretly collecting or sharing private data or location information from the host device.

Although some industry actors have been giving lip service to and others have been really working to establish privacy standards and to provide users with a better understanding of the ways in which their information is used, it seems clear to me that consumers remain in a vulnerable position in which they are required to place an enormous amount of blind trust in online companies and app developers.

Just last week the FTC announced an $800,000 settlement with Spokeo, a data broker that compiles vast amounts of information on consumers from both online and offline sources. In the first FTC case to address the sale of data from the Internet and social media sites in the employment context, the FTC charged that Spokeo violated the Fair Credit Reporting Act by marketing consumer profiles to recruiters and human resource professionals without regard to the accuracy of information and without advising the users how their information would be used. The FTC was empowered to act because of the protections contained in the Fair Credit Reporting Act.

The FTC settlement was announced just as President Obama signed an Executive Order to let the morass of Federal policies and practices that impede broadband deployment on Federal lands. The Executive Order will not only lower the cost of broadband Internet access, it will also speed the delivery of connectivity to communities, businesses and schools. President Obama said in his statement, quote, "By connecting every corner of our country to the digital age, we can help our businesses become more competitive, and our students become more informed, and our citizens become more engaged," close quote.

With greater access comes the responsibility to ensure that our citizens enjoy an online experience that is safe, reliable and respectful of personal information. So I support the direction the Administration is taking us, and continue to believe that Congress should enact baseline privacy legislation that will provide certainty to both consumers and companies, and promote a healthy online economy.

Justice Thurgood Marshall wrote years ago that, quote, "Privacy is not a discrete commodity possessed absolutely or not at all," close quote. The devil is always in the details, but I hope that the witnesses will be able to address some of the best practices recommended by the FTC.

Finally, I am also concerned that without a baseline set of principles with the force of law, privacy policies may be used by larger players in an anticompetitive manner to drive smaller players and start-ups from the market to the detriment of online consumers. I look forward to hearing from our witnesses about how we can embrace new technologies without discarding or abandoning the right to privacy.

And I yield back, Mr. Chairman.

Mr. GOODLATTE. The Chair thanks the gentleman and is pleased to recognize the Chairman of the Judiciary Committee, the gentleman from Texas, Mr. Smith.

Mr. SMITH. Thank you, Mr. Chairman.

America's economic success has been built on innovation. Ten years ago there was no such thing as Facebook or Twitter. Just 5 years ago there was no such thing as an iPhone or an app store. Today, mobile apps number in the hundreds of thousands and are largely developed by individual innovators and small businesses.

As new technologies have emerged, like mobile apps, social media, online advertising and data analytics, the cost for new business entry have come down. But as new Web sites and apps are developed, companies must work to ensure that they maintain the trust of their customers.

Trust is the essential element for consumers to adopt new apps or technologies. When we hear about privacy breaches, like what happened when Google collected large amounts of private data over Wi-Fi networks, we have to be concerned. With every overcollection of privacy data, the first excuse is that the engineers or programmers went beyond what they were told to do. That excuse may fly once, but ultimately it is neither the engineers' fault nor the programmers' fault, it is the company's.

In the Internet economy, online services are generally provided to consumers at little or no cost, and behind these online services

are hundreds or thousands of employees and millions of dollars in hardware and equipment. The Internet economy runs on data. There is an implicit bargain between an Internet service and the consumer that includes an exchange of information or data instead of cash. When a consumer receives a free email account or a cloud storage space, or uses a search engine, social media Web site or app, there is a collection of data that allows a company to construct their service and provide targeted advertising or related data-analytic services to the consumer.

As Internet companies have developed new technologies, their privacy policies have had to evolve. Many companies now institute privacy by design, where privacy protections are built directly into their software and hardware products from the beginning.

Incorporation of the best practices for privacy is essential as new products are developed online. For example, I read that Google and Apple are building even more detailed maps that rival defense satellite imagery. Though this ensures that we will never get lost if we drive or walk through a new city, we also need to ensure that when images are taken in residential areas or in people's backyards, that their privacy is protected. This is another place where privacy concerns should not have to be raised by Congress or the media. They should be addressed before the products are even announced.

The growth in smartphone use and mobile apps has created an entirely new business sector, from Instagram to new mobile apps for established online Web sites and companies. This new business sector is composed mostly of small businesses and individual programmers. As we will hear from our witnesses today, many of these small businesses are just a couple of software programmers, not two programmers and a lawyer, and so they often need assistance from more established players as they work to incorporate privacy protections into their software.

The mobile and Internet playing field is broad, and the specific technological protections may be unique to particular technologies, but as companies incorporate privacy protections into their services, it is important for them to provide privacy policies that are understandable and reasonable. This way it is clear to the consumer what the bargain is that they enter into when they use a Web site or mobile app.

I look forward to hearing from all of our witnesses today, and I hope their testimony allows the Subcommittee to learn how the technology industry works to incorporate balanced privacy protections that will inform and protect consumers.

Thank you, Mr. Chairman. I yield back.

Mr. GOODLATTE. Thank you, Mr. Chairman.

I am now pleased to recognize the gentleman from Michigan, the Ranking Member of the Judiciary Committee, Mr. Conyers.

Mr. CONYERS. Thank you, Chairman Goodlatte and Ranking Member Watt.

This is a very important hearing, and there are new services being offered online and through smartphones and other devices that largely depend on the continued gathering and use of personal information which is ultimately turned into a product for sale. And this hearing is going to devolve, I think, into an issue of whether

we get the self-regulation theory advanced, we will all be good and trust this Committee, or whether we are going to go along and develop the Consumer Privacy Bill of Rights. And that is where we are going to end up, because there is an explosion of the collection, dissemination of personal information, and therefore these organizations have an incentive to collect as much data as possible about Internet users.

And what I think should come out of this hearing is the notion that consumers deserve to know how their data and privacy are being impacted by mobile and online platforms. Today we don't know that. And that is why this hearing by this Subcommittee is extremely important.

The size and power of online companies allow them to obtain and aggregate many types of personal information. Otherwise why would Facebook be valued at a worth of over $100 billion? Well, the answer in large part is because of the treasure trove of personal information that they collect, much of which, like other companies, we don't know much about.

Now, we have been dealing with the size and power of online companies that allows them to obtain and aggregate all this personal information about users. Google recently has had to change its privacy policies, and there is concern about its ability to obtain information through an individual's use of various products the company offers. There are so many different ways to get this information out there, that when they get it together, they have far more information than is generally recognized.

And so I, for one, am interested in learning how we can increase the authority and the power of the Federal Trade Commission to take action against privacy violations. The FTC, in my view, needs direct enforcement authority so that it may take action against those who violate consumer privacy even if a company doesn't violate its own published private policy.

And while companies should develop online guidelines, we must remember that enforcement is critical to consumer protection. The FTC has the responsibility to ensure that competitors are not allowed to play by different rules.

And so, Mr. Chairman, thank you for allowing me to add my comment before the witnesses begin.

Mr. GOODLATTE. I thank the gentleman for his comments.

Without objection, other Members' opening statements will be made a part of the record.

We have a very distinguished panel of witnesses today. Each of the witnesses' written statements will be entered into the record in its entirety, and I ask that each witness summarize his testimony in 5 minutes or less.

To help you stay within that time, there is a timing light on your table. When the light switches from green to yellow, you have 1 minute to conclude your testimony; and when the light turns red, well, that is it. It signals the witness' time has expired.

Before I introduce our witnesses, I would like them to stand and be sworn, as is the custom of this Committee.

[Witnesses sworn.]

Mr. GOODLATTE. Thank you very much, and please be seated.

Our first witness is from the district of the gentlewoman from California, Ms. Lofgren. And so it is my pleasure to yield to her for the purpose of introducing Mr. Shipman.

Ms. LOFGREN. Well, I thank you, Mr. Chairman, for your courtesy in allowing me to introduce the Associate General Counsel of eBay that is, in fact, located in the 16th Congressional District. Scott Shipman has been with eBay from the beginning. In fact, he started at eBay when he was a law student. And the one lawyer there was absolutely overwhelmed, and so he was there at the beginning to deal with the privacy policies of eBay, and he is here to tell us about those successful policies. As he said at our collective law school, he had done the right things without even knowing it back as a law student.

He now has firsthand experience with the privacy compliance and risk assessments at eBay; the cross-border data transfers, including the EU; the personal information transfers through corporate mergers and acquisitions; and all the other privacy-related issues that this major corporation faces.

He teaches international data protection at Santa Clara University School of Law as a lecturer, and he serves along with me on the high-tech law advisory board at our mutual alma mater Santa Clara Law School. He coordinates the legal high-technology internship program at eBay in connection with Santa Clara Law School, and he is a board member of the Consumer Privacy Law Forum. He is a member of the International Association of Privacy Professionals, a member of the Chief Privacy Officers Council, on Conference Board, as well as, of course, being admitted to the California State Bar. I am so glad he is here to share his expertise with us.

And it is good to welcome you here, Scott, from the Valley and to D.C.

Thank you, Mr. Chairman, for allowing me to introduce Scott.

Mr. GOODLATTE. Thank you, Ms. Lofgren.

And I have had the pleasure of speaking at the State of the Net West Conference, which has been hosted at the Santa Clara University School of Law on a number of occasions.

So, Mr. Shipman, welcome.

Our second witness is Mr. Morgan Reed, Executive Director of the Association for Competitive Technology. Mr. Reed specializes in technology issues and has been working closely with mobile app developers and companies on privacy issues for years.

Mr. Reed previously worked for a Taiwan-based trading company handling North American sales operations. He received his B.A. in Political Science from Arizona State University, and did graduate research in Chinese at the University of Utah and the Shi Ta University in Taiwan. I hope I have that pronounced correctly.

Mr. REED. Close enough.

Mr. GOODLATTE. Our third witness, Mr. Chris Babel, is the CEO of TRUSTe, a leading company and authority on Internet trust and privacy. Previously Mr. Babel served as Senior Vice President and General Manager of VeriSign's worldwide authentication services business, where he was responsible for strategy, sales, marketing, product and support. He also managed VeriSign's SSL and Managed Security Services business. Earlier in his career he worked at

Morgan Stanley in their M&A and Corporate Finance group. Mr. Babel received his B.A. in Mathematical Methods in Social Sciences and Economics from Northwestern University.

And our fourth witness is Mr. James Grimmelmann, professor of law at New York Law School. Professor Grimmelmann studies technology issues relating to IP, virtual worlds, search engines, online privacy and other topics. Prior to law school he worked as a programmer for Microsoft. He received his J.D. from Yale Law School and his A.B. in Computer Science from Harvard College.

Welcome to you all. And we will begin with Mr. Shipman.

TESTIMONY OF SCOTT R. SHIPMAN, ASSOCIATE GENERAL COUNSEL, GLOBAL PRIVACY LEADER, eBAY INC.

Mr. SHIPMAN. Chairman Goodlatte, Ranking Member Watt and Members of the Subcommittee, thank you for the opportunity to testify today about eBay Inc., and what we are doing to enable commerce and engender trust through the use of innovative consumer privacy protections. My name is Scott Shipman, and I am the associate general counsel and global privacy leader for eBay Inc.

eBay empowers and connects millions of buyers and sellers throughout the globe through eBay marketplaces, Paypal, GSI and other mobile technology-based businesses; therefore, many people associate eBay and Paypal with enabling e-commerce. However, it is important to note that eBay is not just about e-commerce. We are about commerce.

The traditional boundaries of offline and online retail are blurring. We recognize that retailers and sellers of all sizes need a partner who will help them succeed in this rapidly changing, consumer-driven environment. We want them to succeed, and we are that partner.

Over the years we have learned one of the keys to success is engendering consumer trust and confidence. A critical component of that trust is privacy. It is hard to build consumer trust when you are not respectful of their personal information. To foster that trust we have had to meet customer privacy expectations with every product we offer. I would like to take the next few minutes to highlight some of the successful privacy-related programs and products that have led to eBay being rated one of the most trusted companies for consumer privacy.

Since eBay's inception our core privacy commitment is eBay will not sell the personal information of our customers to third parties for marketing purposes. However, we also recognize consumers need more meaningful choices on how their data was used for behavioral-targeted advertising; therefore, eBay developed and implemented a program called AdChoice.

The AdChoice program works as follows. Third-party advertisements on and off eBay have an AdChoice link. When eBay users click on the link, they see a pop-up window that gives them the ability to specify their advertising preferences. eBay users can also opt out of receiving third-party behaviorally targeted ads and read our privacy policy through that link.

eBay's AdChoice program offers a server-based mechanism, not their traditional cookie-based mechanism. This means choices and

preferences are permanently stored and not erased when a user clears their cookies.

Paypal and its "shop without sharing" design is another perfect example of innovative technology that encourages consumer privacy and consumer control. The beauty of Paypal is it allows consumers to pay for a good or service without ever having to expose their credit card or bank account information to merchants. Not only does this privacy-enhancing technology allow consumers to fully enjoy the convenience of online and mobile commerce, but it also allows merchants to receive payments without the cost and potential liability associated with processing and securing financial information. It is a win-win for both consumers and merchants.

Looking now at the exciting mobile space, mobile applications and technology continue to grow in popularity and importance. Through the launch of several new and exciting mobile applications, eBay has experienced rapid growth in the mobile arena. However, being a leader in mobile and geolocation technology is more than just offering cool new services; it is also about balancing the needs and wants of the consumer against the creep factor that is sometimes associated with the collection and use of geolocation and mobile data.

eBay is building mobile applications that offer the same transparency, choice and level of privacy protection as our traditional Internet services. eBay has made it a policy that all consumers must opt in to turn on geolocation for all eBay Inc., mobile applications, and we give consumers the ability to decide what communications and notifications they want to receive and how.

A perfect example of an eBay mobile application that encapsulates the privacy by design philosophy is WHERE. WHERE provides personalized hyperlocal recommendations, offers and deals to millions of mobile consumers. WHERE does not associate personally identifiable information with location data without explicit consent. Finally, WHERE does not collect, maintain or track a consumer's location history.

I have talked a lot about technology, but my last example focuses on best practices and compliance. In addition to eBay's privacy principles and the practices described in our privacy policies, eBay has established a set of corporate rules approved by the Luxembourg National Data Commission. These corporate rules are a commitment by eBay to protect our users' personal information regardless of where the data resides.

Our corporate rules do not just protect the personally identifiable information of our European users, but of all eBay Inc. customers and employees globally. eBay was actually the first e-commerce company to receive this approval and the first company to receive approval for employee and customer rules.

To conclude, we recognize that privacy is a key component of our customers' experience and the trust they place with us. As technology changes, as the world changes, expectations will continue to change. eBay's role is not to guarantee absolute privacy in a vacuum, but to build a relationship based on trust. It is our hope that in the years to come, the trust within that relationship will only grow stronger, and our customers will know and trust that we will get it done right.

I sincerely appreciate the opportunity to testify before the Committee today, and I look forward to your questions.

Mr. GOODLATTE. Thank you, Mr. Shipman.

[The prepared statement of Mr. Shipman follows:]

Testimony of

Scott R. Shipman

Associate General Counsel, Global Privacy Leader

eBay Inc.

Before the

United States House of Representatives

Committee on the Judiciary

Subcommittee on Intellectual Property, Competition and the Internet

"New Technologies and Innovations in the Mobile and Online Space, and the Implications for Public Policy"

***Presented*:**

Rayburn House Office Building, Room 2141

June 19, 2012

10:00 AM

Chairman Goodlatte, Ranking Member Watt, and Members of the Subcommittee: Thank you for the opportunity to testify today about eBay Inc. and what we are doing to enable commerce and engender trust through the use of innovative consumer privacy protections.

My name is Scott Shipman and I am the Associate General Counsel and Global Privacy Leader for eBay Inc. Founded in 1995 in San Jose, Calif., eBay Inc. connects millions of buyers and sellers globally on a daily basis through eBay, the world's largest online marketplace, and PayPal, which enables individuals and businesses to securely, easily, and quickly send and receive online payments. We also reach millions through specialized marketplaces such as StubHub, the world's largest ticket marketplace, and eBay classifieds sites. Currently, we have

over 102 million users worldwide and in the first quarter of 2012 alone over $16 billion in goods were traded on our site.

Additionally, eBay Inc. is actively working to revolutionize global commerce with the recent additions of mobile technology companies WHERE, Milo, Zong and others combined with the seasoned services of eBay Marketplaces Mobile and PayPal Mobile. In fact, in 2011, eBay Inc. generated nearly $5 billion in global mobile sales, which was a 150 percent increase from the previous year. eBay Mobile also experienced great popularity across the globe, with consumers from over 190 countries worldwide downloading eBay Inc.'s applications 80 million times. Our global consumers bought everything from cars, clothing, shoes, electronics, and toys from eBay's mobile applications.

But eBay Inc. is not just about "E" commerce. eBay is about "Commerce." We facilitate consumers buying just about anything whether on or offline. We enable consumers to pay online, pay with a phone, pay with a card from your wallet or pay with nothing but a phone number and a secure pin.

Current retail trends show that the future of retail is no longer brick and mortar vs. online or eCommerce vs. Commerce. The traditional boundaries between the offline and online marketplace are blurring and soon it will all just be ***Commerce***. All sustainable 21st Century retail business models, large and small alike, will use the Internet and mobile technology tools. In fact, the Census Bureau and Forrester Research show that web-influenced in-store retail will represent almost 40% of all retail in 2012.[1]

With this growing trend in mind, eBay Inc. has evolved its business model to include technology solutions for traditional brick and mortar stores, both large and small. Retailers and sellers of all sizes need a partner who will help them succeed in this new technology-driven environment, and who will not compete with them. We are that partner.

[1] Forrester Research: Web-Influenced Retail Sales Forecast 2010-2015 (US).

Through our company GSI Commerce, eBay Inc. has become the leading provider of eCommerce and interactive marketing services for many of the world's premier brands and retailers, such as Toys R Us, Ralph Lauren and Dick's Sporting Goods. In addition, our recent launch of PayPal Here, a mobile payment solution, is designed to help small businesses accept almost any form of payment from almost anywhere.

eBay Inc. is a very diverse family of businesses supporting millions of users ranging from individual consumers to merchants and retailers of every shape and size. Over the years we have learned that one of the keys to success is engendering consumer trust and confidence. It is our belief that without trust, the Internet and mobile marketplaces will fail to reach their full potential. Privacy and trust are mutually reinforcing. It is hard to build consumer trust when you are not respectful of a consumer's personal information.

To foster that trust, we've had to meet customer privacy expectations with every product we offer. Even before "privacy by design" was a popular, mainstream concept, eBay made privacy expectations a fundamental building block of our products and services. It is my job to ensure that we continually strive to meet and exceed consumer expectations, while offering greater levels of transparency, consistency, and consumer control. I'm proud to report that as a result of our focus on privacy, eBay Inc. was twice ranked by consumers as the most trusted brand for privacy through the Ponemon Institute[2].

I would like to take the next few minutes to highlight some of the successful privacy-related programs and products that have led to eBay Inc. being rated one of the most trusted companies for consumer privacy.

AdChoice

eBay Inc. has consistently been an Internet industry leader in advocating for strong privacy protections and consumer control. Since eBay Inc.'s inception, our core privacy

[2] Survey Conducted by Ponemon Institute and TRUSTe in September 2009. See www.truste.com, Press room, Archives, September 16, 2009 : 2009 Most Trusted Companies In Privacy Announced

commitment has been that eBay will not sell the personal information of our customers to third parties for marketing purposes. However, we also recognized that a mechanism was needed to provide consumers with more meaningful choices over the way their aggregate anonymous data was used for behaviorally targeted advertising purposes. Years before there were any industry wide solutions, eBay developed and implemented a program called AdChoice. AdChoice allows eBay users to choose whether to receive behaviorally targeted third party advertising on eBay and on the websites of our advertising partners.

The AdChoice program works as follows: third party advertisements on and off eBay powered by our behavioral targeting engine have an AdChoice link. When eBay users click on the link, they see a pop-up window that gives them the ability to specify their advertising preferences, opt-out of receiving third party tailored ads, and read our privacy policy.[3] It is important to note that eBay's AdChoice program offers a server-based mechanism, not the traditional cookie-based mechanism, which means choices and preferences are permanently stored and not erased when a user clears their cookies.

[3] eBay's Privacy Policy: http://pages.ebay.com/help/policies/privacy-policy.html

Since the launch of our AdChoice technology in 2007, at the Federal Trade Commission's "Ehavioral Advertising" Town Hall, eBay Inc. has received positive feedback from consumers, lawmakers, and fellow industry leaders. In fact, our AdChoice program has been so successful that in October of 2010, a group of major marketing and media companies launched a similar program, which endorsed the use of the "Advertising Option Icon." The "Advertising Option Icon" is displayed within or near online advertisements or on Web pages operated by members of the participating entities. However, the industry solution is still cookie-based and not persistent like the server-based AdChoice program.

eBay Inc. believes that programs like AdChoice not only give consumers greater choice and control over the use of their information for behavioral advertising, but also foster an environment that allows companies to innovate and create new technological solutions that could surpass current models.

PayPal: Shop without Sharing

PayPal and its "shop without sharing" design is another perfect example of innovative technology that encourages consumer privacy and consumer control. PayPal is an eBay Inc. company that acts like a digital wallet where you can securely store all your payment options, such as your bank account and credit card. When you want to make a payment, you don't have to pull out your credit card or type your billing information every time. With 110 million active registered accounts in 190 markets and 25 currencies worldwide, PayPal is enabling global commerce and providing a faster, safer way to pay and get paid online.

Privacy is one of the fundamental building blocks of the PayPal services. The beauty of PayPal is that it allows consumers to send money or pay for a good or service without ever having to expose their credit card or bank account information to merchants or other PayPal users. It allows consumers to shop online or on their mobile device without having to share the most sensitive personally identifiable information, financial and banking information. Not only

does this privacy-enhancing technology allow consumers to fully enjoy the convenience of online and mobile commerce without worrying about safety and security concerns, but it also allows merchants to receive payments without the cost and potential liability associated with processing and securing financial information. We believe enabling consumers to pay merchants without sharing their financial information is the ultimate 'privacy by design' financial service. Notably, this PayPal design has been a key feature of PayPal since its inception. It's a win-win for both consumers and merchants.

However, PayPal's technology is only part of our overall efforts to encourage greater privacy awareness and protection. PayPal also provides an extensive security education center for consumers to learn how to protect their personal and financial information online. We not only want to partner with consumers and merchants to enable global commerce, but we also want to partner with our users to ensure safe and secure shopping experiences.

Mobile and Geo-location Technology

Mobile applications and technology continue to grow in popularity and importance, not only to society, but to commerce as well. Due to the technology's flexible and transient nature, mobile has truly become the next commercial frontier. Recognizing early on that customers wanted access to our services anytime and anywhere, eBay Inc. quickly "mobilized" to meet our users' growing demands for new and innovative mobile services. Through the launch of several new and exciting mobile applications that offer a multitude of mobile commerce and payment services, eBay Inc. has experienced rapid growth in the mobile arena.

However, being a leader in mobile and geo-location technology is more than just offering cool new services. It is also about balancing the needs and wants of the consumer against the "creep" factor and sensitivity of geo-location and mobile data. We want to delight customers, provide consumers with the services they desire, such as local advertisements, saved history of offers, and location information on their favorite places, and we want to accomplish this in a way that does not go against consumer expectations for privacy.

Therefore, eBay Inc. is building mobile applications that offer the same transparency, choice, and level of privacy protection as our traditional Internet platforms. In fact, we believe that mobile technology may be able to communicate privacy policies in an even more transparent manner than traditional Internet platforms. We want our users to have the same level of confidence and trust in our mobile services as in our online services. In order to further these efforts, eBay has made it a policy that all consumers must opt-in (rather than opt-out) to turn on geo-location for all of eBay Inc. mobile applications. And we give consumers the ability to decide what communications and notifications they want to receive and how.

A perfect example of an eBay Inc. mobile application that encapsulates the "privacy by design" philosophy is WHERE. WHERE, which is the leading location media provider in North America, provides personalized, hyper-local recommendations, offers, and deals to millions of mobile consumers. More than 120,000 retailers, brands and small merchants use these services daily to reach new audiences and deliver real-time foot traffic to their doorstep. And for consumers, WHERE helps users discover, save, and share their favorite places by putting the best local information at their fingertips and offering great deals from nearby businesses.

Even before we acquired WHERE in 2011, the company was a leader in mobile privacy. WHERE made it a policy to:

- Only collect information insofar as necessary or appropriate to fulfill the purpose of the user's interaction;
- Not associate personally identifiable information with location data unless given express permission;
- Not collect, maintain or track location history;
- Not share personally identifiable information with third parties or service providers.

eBay Inc. remains committed to continuing the privacy tradition of WHERE, and as mentioned earlier, we have now made it a standard practice that **all** consumers must opt-in to turn on geo-location for **all** of eBay Inc. mobile applications. Mobile and geo-location services

are the future of commerce, and as an industry leader, we want to ensure that we are setting the bar high in order to build the trust that is necessary for the long-term success of this technology.

Binding Corporate Rules

I have spent a lot of time discussing what we do from a technological perspective to protect consumer data. However, I wanted to spend the last few minutes of my testimony discussing our implementation of a voluntary global corporate compliance strategy, which we have undertaken in order to ensure we can live up to the trust we seek from our customers worldwide.

In addition to eBay Inc.'s privacy principles and the practices described in our privacy policies, eBay Inc. has established a set of Corporate Rules (also referred to as Binding Corporate Rules), approved by the Luxembourg National Data Commission.[4] These Corporate Rules are a commitment by eBay Inc. to protect our users' personal information regardless of where the data resides. It is important to note that our Corporate Rules do not just protect the personally identifiable information of our European users; we have made the decision as a company to apply these privacy protections to the personal information of all eBay Inc. customers and employees globally. eBay Inc. was actually the first eCommerce company to receive this approval and the first company to receive approval for employee and customer rules.

Conclusion

To conclude, eBay Inc. is committed to delighting our customers and exceeding their expectations at every turn. We recognize that privacy is a key component of their experience and the trust they place with us. As technology changes, as the world changes, expectations will continue to change. My role is to keep up with those changing expectations and help eBay Inc. surpass the bar that our consumers and employees challenge us to reach on a daily basis. eBay Inc.'s role is not to guarantee absolute privacy in a vacuum, but to build a relationship based on

[4] eBay Inc.'s Corporate Rules: http://www.ebayprivacycenter.com/privacy/binding-corporate-rules

trust. It is our hope that in the years to come the trust within that relationship will only grow stronger because our customers will know and trust that we will treat them with respect and we'll get it done right.

I appreciate the opportunity to testify before the Committee, and I look forward to your questions.

Mr. GOODLATTE. Mr. Reed, welcome.

TESTIMONY OF MORGAN REED, EXECUTIVE DIRECTOR, ASSOCIATION FOR COMPETITIVE TECHNOLOGY

Mr. REED. Thank you.

Chairman Goodlatte, Ranking Member Watt, Members of the Committee, my name is Morgan Reed, and I want to thank you for having today's hearing on New Technologies and Innovations in the Mobile and Online space and the Implications for Public Policy.

My organization, the Association for Competitive Technology, is an international trade association representing more than 5,000 app developers. We make the cool apps that run on your smartphone, and your iPads, and, hopefully, the new Microsoft tablet and the next device after that. I am a licensed developer, too, having worked on network protocols and debugging games, so I have actually dug into the nitty-gritty of how you build software programs.

Here is the great news: Our industry is showing amazing growth. We have hit more than $20 billion today on an expected path to $100 billion by 2015. Apps are expanding into new markets, including enterprise and mobile health, which will help make Americans more efficient at work and healthier at home. And while Americans own more than 350 million mobile devices, developers are seeing real potential in foreign markets. China's largest telecommunications company has more than 800 million subscribers; the number 2, 200 million; the number 3, 100 million. With adequate intellectual property protection, those subscribers could become customers for our American developers.

Now, I understand this Committee would like to spend some time today talking about consumer data privacy and how we make it work in this new, more mobile world. What we have learned in working through several multi-stakeholder efforts is that we need to address privacy in a comprehensive way, not one that creates siloed solutions for each technology, especially since those silos are disappearing every day.

The biggest revolution in our industry is happening right now, and it is called responsive design. Technology is giving us the tools to make one app that will look good on a mobile device and will also look good on a television, and it will do so seamlessly.

Everyone in the technology industry has to take part and be responsible for improving the state of privacy security and transparency across all of these industries and devices. Our app developers are no different, and we are committed to working this out with government, industry, civil society and, most importantly, our customers.

During the past year ACT has reached out to our membership and other developer organizations throughout America to discuss the importance of data privacy. We have gone coast to coast and have reached hundreds of thousands of developers. Our message has been simple: know what data you are collecting, know who you are sharing that data with, and be transparent with your customers.

We have also been participating in multi-stakeholder efforts, including the California AG's work on mobile platforms and the White House's NTIA multi-stakeholder effort.

But throughout all this talk about stakeholders, I realize that this can easily be seen to imply large, faceless corporations. I wanted you to remember today that the incredible innovation happening is being driven by thousands of small businesses working to build applications that educate, motivate and enrich people's lives. Therefore, I thought I would take a minute to introduce you to some of the stakeholders whose voices we are working to have heard throughout these efforts.

Chairman Goodlatte, in your district Vision Studios produced TextGauge. It is an app for parents to prevent teens from texting while driving.

Congressman Watt, in your district we have got Monster Physics. It is a great app that makes physics fun and is available for adults as well as kids.

Congressman Conyers, in your district JacAPPS is building the app for the Detroit International Jazz Festival. It is an amazing application.

Congressman Smith, in your district My Patient Solutions helps patients navigate the health care system by giving them tools to better understand diagnosis and treatment options.

Congressman Marino, we have social meetup apps done by MeetMe! in your district.

Congressman Quayle, in your district we have a brand new entrant. ABN just won the contract for the 2012 PGA Phoenix Open, and that will have location-based technology to allow you to go on-the-ground navigation with the spectators.

Congressman Deutch, in your district one of our members, Dave Noderer, built an app for Big Brothers and Big Sisters that allows Bigs to know activities that they should be looking at doing with their Littles.

Congressman Griffin has OrderPath. It allows medical personnel to display in-patient and observation data to help streamline patient care, and it is aimed at rural districts.

Congresswoman Chu, in your district Awesome App; it is for electricians and engineers that helps them do their job more efficiently and, importantly, more safely.

Congressman Chaffetz, you have got one of the biggest dogs in the fight. Infinity Blade II is built in your district, millions of downloads, and it is built by a very small company right in your district.

Congresswoman Lofgren, we have got a great app in Pinger. It allows people to send free text messages all across the world without having to necessarily have a specific text plan.

Congressman Poe has got iTaxable that provides answers to your tax filing questions and an extensive database of information.

Congressman Jordan, you have got Ranch Rush. It is a game that puts a farm in your pocket, allowing users to harvest fresh produce, gather eggs from ostriches, collect honey from bees, and whip up ketchup from tomatoes.

Congressman Nadler has got one that helps you sign your signature on your iPad instead of having to find a fax machine.

So I think as we think about today's questions about stakeholders, you need to remember that in every single one of your districts, and in every district here in Congress, there is a small business stakeholder whose voices we need to have heard as part of this privacy discussion.

Thank you for your time, and I look forward to your questions.

Mr. GOODLATTE. Thank you, Mr. Reed.

[The prepared statement of Mr. Reed follows:]

-

Testimony

of Morgan Reed
Executive Director
The Association for Competitive Technology

before the
Committee on the Judiciary
Subcommittee on Intellectual Property, Competition and the Internet
on
New Technologies and Innovations in the Mobile and Online Space, and the Implications for Public Policy

June 19, 2012

Chairman Goodlatte, Ranking Member Watt, and distinguished members of the Committee: My name is Morgan Reed, and I thank you for holding this important hearing examining innovations in the online space and the implications for public policy.

I am the executive director of the Association for Competitive Technology (ACT). ACT is an international advocacy and education organization for people who write software programs--referred to as application developers. We represent over 5,000 small and mid-size IT firms throughout the world and advocate for public policies that help our members leverage their intellectual assets to raise capital, create jobs, and innovate.

While I am here today on behalf of our members, I am also here representing myself – I am a developer as well. Having worked on projects ranging from Linux networking tools to client/server protocols, I still keep my iOS license up to date, even if I no longer have the cutting edge skills of my younger days.

My goal today is to explain the evolving nature of the mobile application industry, the business challenges we face, and the public policy issues that we encounter. Specifically, app developers have three key messages for the members of the Committee:

1. **The app marketplace is still in its earliest growth stage, rapidly continuing to evolve.**

2. **Our industry is working to expand into new fields including mobile health and to new parts of the world.**

3. **Our public policy challenges include adequate intellectual property (IP) protection abroad, regulatory clarity for new markets, and proper consumer data privacy protection.**

Evolution of the App Marketplace

I spend a significant portion of my time speaking to non-developer audiences who want to know about the state of the mobile apps economy. Unlike other industries, I find that I have to update my numbers for every speech, not just once or twice a year. Just two years ago, total industry revenues were $3.8 billion and expected to rise to $8.3 billion.[1] At the close of last year we had grown to $20 billion and are projected to reach $100 billion by 2015.[2] This is a meteoric rise for an app economy that didn't even exist four years ago.

[1] http://www.eweek.com/c/a/Mobile-and-Wireless/Apple-Google-Lead-38B-Mobile-App-Charge-IHS-512817/
[2] http://www.slideshare.net/joelrubinson/an3-us-appeconomy20112015

The rise of the app marketplace has coincided with the explosive growth of smartphones. Sales of these devices continue to outpace all predictions and are providing a huge boost to our economy. Total smartphone sales in 2011 reached 472 million units and accounted for 31 percent of all mobile device sales, up 58 percent from 2010. In the United States and Europe, smartphones sales have begun to overtake feature phones and that trend is expected to continue.

Smartphones derive considerable value from the apps that run on them. Consumers are attracted to phones based on the functionality these programs provide. Telephone companies and handset makers have devised entire ad campaigns built around highlighting the apps that run on their platforms. "There's an app for that" is probably one of the most recognizable ads in the technology space.

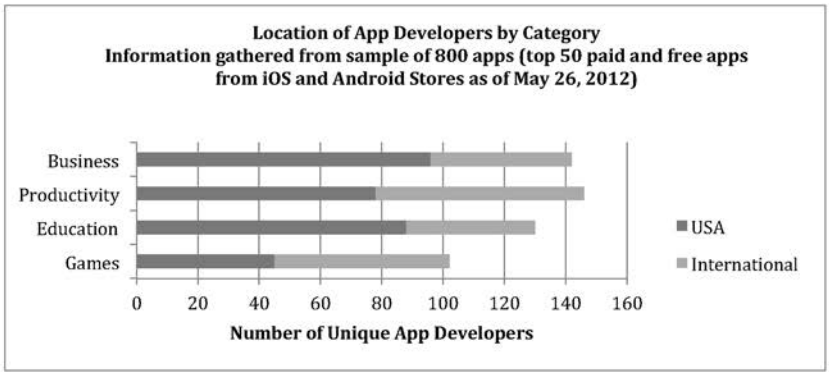
The App Marketplace: An Incredible Success Story

It should come as no surprise that the growth of the app industry has been a dramatic success story, even in the face of our enduring economic slowdown. The mobile app market got started in 2008 when Apple launched its App Store and allowed independent developers to sell applications for the iPhone. Since then, over 30 billion apps have been downloaded in the App Store, earning developers over $5 billion. Over a million apps are now available across all platforms.

This success has had a dramatic impact on job creation. ACT's study in 2011 estimated that the current mobile apps economy has created, saved, or supplemented more than 600,000 jobs nationwide across iOS, Android, Windows Phone 7, and Blackberry platforms. Another study by TechNet showed nearly 500,000 jobs created by the app economy on the major platforms alone.

America's Lead in Mobile Apps Exists, But is Not Guaranteed

ACT has recently completed a new analysis of the current mobile app ecosystem, this time examining apps not only by revenue, but also by type. We looked at the top 800 apps across the Productivity, Education, Business, and Entertainment categories. And in dramatic comparison to our 2010 research, international firms are surging to represent a significant portion of apps for sale. International developers have become strongest in games, an area dominated by products using in-application purchasing, a payment method that didn't even exist in 2010.



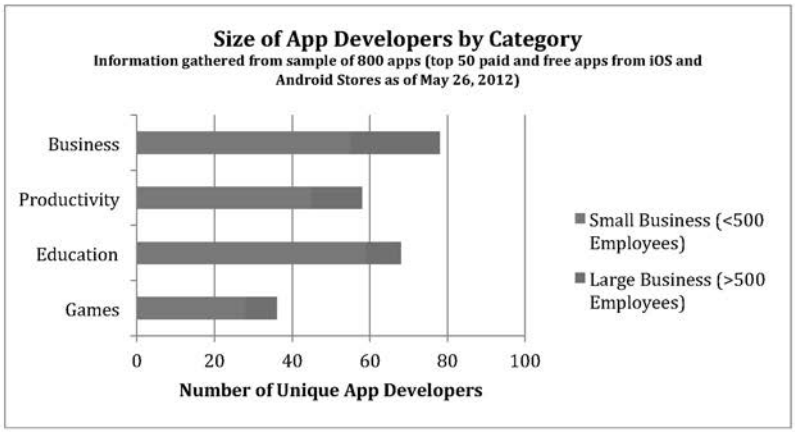
As a brand new industry, we are experiencing rapid changes in the marketplace with new business models emerging every year. Freemium apps and in-app purchasing have become the favored means to monetize new releases.[3] Not long ago, paid downloads ruled the day. Through it all, developers are still exploring whether the advertising model can generate enough income on its own.[4]

While business models continue to evolve, developers are also experimenting with different platforms. Currently Apple's iOS provides the most dependable platform, but RIM has been aggressively wooing developers to Blackberry as its user base in Asia and the Middle East remains strong.[5] Android continues to maintain marketshare, although fragmentation is becoming a serious issue for developers[6]; and just yesterday Microsoft announced the creation of a Microsoft-built mobile tablet with a new Metro style user interface.

Still Small Business Strong

ACT research continues to find that the majority of the top-selling mobile app developers (78%) are small businesses. Nowhere is the dominance of small business seen more than in education apps, where over 70% of the app developers surveyed were small businesses. Of those small businesses, 87% have 50 or fewer employees. The other categories were also predominantly small businesses, though to a lesser degree.

[3] http://www.nytimes.com/2012/03/19/technology/game-makers-give-away-freemium-products.html?_r=1&pagewanted=all
[4] http://tech.fortune.cnn.com/2011/11/21/piper-jaffray-android-app-revenue-is-7-of-iphones/
[5] http://www.engadget.com/2012/02/03/RIM-free-BlackBerry-Playbook-Android/
[6] http://www.reuters.com/article/2012/03/20/mobile-developers-idUSL1E8EJAGT20120320



The category with the biggest number of large companies is Business, due primarily to the number of apps developed by existing large corporations to connect mobile users with their existing services, such as PayPal, UPS, and FedEx. But there's good news even in those numbers. The vast majority of the "large business" apps were not built internally, but were built by small contract developers, like Big sushi in Charlotte, North Carolina, or Found Design+interactive in Harrisonburg, Virginia.

With such a dynamic mobile ecosystem it is difficult to predict where the market is headed next and what industry standards will be adopted. This makes it difficult to implement a regulatory regime for the app marketplace. The industry is far from mature and activities or practices that regulators seek to address may no longer exist in their current form by the time new rules can be implemented.

New Opportunities to Grow Both Domestically and Abroad

While we all know of the explosion of mobile apps and smartphones for consumers, there's another wave of innovation on the horizon. We expect that mobile apps will have a significant impact at the enterprise level over the next 12 to 24 months, with nearly every major corporation and government agency adopting tablet computers directly, or instituting bring your own device (BYOD) policies. This sea change will improve efficiencies and create new workflows inside of corporations, but it also provides real opportunities for developers to expand beyond the 99¢ price point or ad-supported models.

Educators are also exploring the benefits that app-powered tablet devices can have in the classroom. Just a few months ago, the state of Alabama passed legislation that would give every student a tablet to use for books and classwork. The enormous implications of individualized teaching and assistance to special needs kids aside, this will certainly reduce the weight of our children's backpacks!

We also see great potential for mobile apps to lower costs and improve health and healthcare. I'm honored to be on the advisory council for mHIMSS, the mobile initiative of the largest health IT membership association. Through the efforts of ACT and organizations like mHIMSS, we are improving health and healthcare delivery through the use of mobile and wireless technologies. For example, use of mobile devices can help to maximize the value of the $38.7 billion the U.S. government committed to help doctors convert from paper to electronic health records.

Finally, ACT sees opportunity for international growth. The 99¢ price point of apps makes them accessible in developed and developing countries alike. Foreign markets— particularly those in Brazil, Russia, India, and China— offer considerable opportunities for our members. The BRIC nations produce more than 50% of the revenues for the technology industry and offer far more in growth opportunities. In looking at the top 50 paid iOS apps in China we found reason to cheer. While the market is predictably dominated by apps made in China, 23% of the apps in the top 50 were made by U.S. app developers. For example, tap tap tap, a U.S. app developer based in San Francisco, California, created the app Camera+ which was the 35th most popular paid app on the Chinese iOS app store. A small business with only 16 employees, tap tap tap has sold over 8 million Camera+ apps world-wide since it was released on June 7, 2010.

Rapid Growth and Rapid Response to Public Policy Questions

For app makers, our public policy concerns fall into three basic categories: making sure our property rights are respected, lowering barriers to entry, and finding ways to educate our customers about the acquisition, use, and storage of data they may consider private or could affect their daily lives.

International Opportunities Have New Risks

While piracy has historically posed a challenge for developers across the world, the emergence of mobile app stores has offered a partial reprieve. Apple, Microsoft, and Blackberry sell apps in curated stores. Phone users can only install apps through a store that reviews each piece of software before approving its admission. Although some developers chafe at the control these stores exert and the conditions required

in the approval process, they largely appreciate that stores greatly cut down on the piracy rate.

Each app installation from a curated store—even free apps—involves a transaction record. This has cut down on pirated sales, relegating them to open platforms such as Android where they proliferate as free downloads. It is still possible to hack phones to provide access to alternative app stores where pirated apps can be found, but this involves technical expertise and voids the terms of service. Since this action denies the user access to technical support, upgrades, and virus protection, most Americans opt not to pursue this illicit route.

In China, however, this has not been the case for multiple reasons. The incidence of hacked or "jailbroken" phones is high with estimates as great as 60%. Combined with China's traditionally lax enforcement of intellectual property rights, U.S. developers' export opportunities are limited at a time they should be rising.

Healthcare Needs Disruptive Change, but Not at the Cost of Safety
App developers have seen enormous growth in the healthcare space, but confront significant barriers to entry created by regulatory rules that have not kept pace. HIPPA is a critical regulation for protecting the privacy of patients, but its implementation can create challenging barriers for the display and storage of a patient's information, barriers which neither enhance care, nor privacy protection.

FDA regulations governing what app is, and isn't, a medical device have been slow to materialize. We are cautiously optimistic that the FDA will publish its final guidance soon, and we expect it will take the "light touch" approach specified by Dr. Jeff Shuren, the FDA's director of the Center for Devices and Radiological Health.

Finally, the byzantine schedule of payment codes presents challenges, as developers find ways to demonstrate how their products replace an existing product listed in the code, even when the feature-set of the new mobile product is far more capable and can be priced much more inexpensively. Worse still is the battle to describe an innovative new product in a way that matches old, pre-mobile concepts. It can be akin to describing a modern car in terms originally created for horse and buggy.

All of this must be accomplished in a way that continues to place efficacy and patient safety first and new technologies second. We look forward to embracing the challenges; it will take time, research, the collaboration of industry and academia, and possibly help from Congress.

Privacy: It's All About the Data

As the app marketplace is experiencing dramatic expansion and innovation, concerns for consumer privacy online have grown. While most of the headlines have been earned by big companies operating in traditional Internet commerce (the Google wi-spy case is still raising public ire), the app industry has not been immune

from privacy missteps. Most famously, Path failed to inform and educate its customers before changing the way it collected and stored user contacts. Path was excoriated in the press, and deleted all data collected after making very public amends.

However a great deal of the overall tension surrounding privacy comes from the practical requirements that companies collect, and occasionally share, data.

For example, a huge reason for the success of the mobile app ecosystem has been the ability of developers to focus only on the truly innovative parts of their product; by using third parties to provide features like analytics, networking, and payment processing, developers have been able to build amazing products with low overhead and instant responsiveness.

And this offloading of overhead can even have positive privacy implications. It's well known that Apple collects credit card information and does not share it with developers, but for those not on the Apple platform, companies like PayPal provide a way for consumers to pay without sharing. The fact that customers trust PayPal actually increases the user's comfort with paying for a mobile app without having to wonder where his financial data will end up. PayPal reduces risk for both developers and consumers.

For advertising, Apple's iAd is a "black box" that provides no private user data to developers, and several Interactive Advertising Bureau (IAB) member companies have "share aggregate data only" policies that prevent sensitive data from being sent back to the developer.

The fact that third party sharing of data is both a business necessity and can enhance consumer data safety does not preclude industry from taking privacy seriously. In fact the only way we can maintain and build on consumer trust is to continue to take it seriously, and urge enforcement actions against companies that violate the public trust.

The good news is that a huge number of industry groups and individual companies have been creating tools and guidelines for helping educate consumers, developers, and regulators alike, knowing full well that if we don't, we face the loss of consumer trust, and possible legal action.

These industry- and advocate-created guidelines generally take a multi-layered, multi-level approach, because there quite simply cannot be a single answer. Consumer data is collected through a number of different methods and technology platforms. It can occur on a website, a mobile device, or most commonly a point of purchase sales transaction at a bricks and mortar store. Your grocery rewards card knows what kind of milk you like, a website might be aware of your interest categories, and a mobile app may be location aware to give you better mapping

information. And in each of these examples the information may, or may not, be shared with other participants in the ecosystem.

Because data arrives from so many different kinds of technology, privacy efforts must be focused around data, rather than the technology used to collect.

Industry Efforts on Privacy Span All Boundaries
In order to deal with privacy from a data perspective, rather than a technology one, industry groups have been developing guidelines and best practices for dealing with information, from private, sensitive data to anonymous, aggregate numbers that specify no single person.

Within the Internet ecosystem, numerous trade associations, including ACT, and advocacy groups have pulled together guidelines and best practices. Generally these guidelines strive to be technology agnostic, based around overall industry sectors or business models.

A quick review of some of these include:

- *From the telecommunications industry, GSMA and CTIA/ESRB both have guidelines for providers and developers, and CTIA/ESRB has content ratings that include separate privacy notifications.*
- *For advertisers, NAI, DAA, IAB, DMA, WOMMA, MMA, and others have guidelines for advertising companies, notifications for consumers (the forward "i"), and even best practices for app developers.*
- *For retail companies, the Electronic Retailers Association, the National Association of Retailers, and the Better Business Bureau have information on how retailers should and should not collect and share data.*
- *Advocacy groups like EFF, Public Knowledge, CATO, Mercatus, and others have extensive blog posts, write-ups, and in some cases developer guidance for dealing with consumer information.*
- *Not to be left off the list, the American Bar Association has weighed in, especially through the Federal Communications Bar Association, which has held workshops, created papers, and hosted multi-stakeholder summits at their annual meeting.*

Still other groups, like the Family Online Safety Institute (FOSI) and the Center for Democracy and Technology (CDT) have worked as conveners for multi-stakeholder efforts.

How Do We Get the Message to Developers?
For ACT, we have taken an aggressive two-stage approach. Of course we've developed guidelines and best practices, but we've decided that the most important

role we can play is that of educating our developers about their roles and responsibilities in the overall ecosystem.

We believe the biggest hurdle to implementing industry-wide privacy standards is developer education. There are over 200,000 app developers in the United States. App makers want to do the right thing on privacy, but often don't know whether their app creates privacy concerns or what they need to do to be rules compliant. As most small business app developers are making customer-facing software for the first time, they are also addressing privacy issues for the first time. Matters typically handled by a legal department or chief privacy officer in a larger company are now most often handled by a small business owner.

In order to meet this demand, ACT has undertaken an ambitious developer campaign, one that has put us in front of thousands of developers all across the country. Here are just a few highlights:

- *Privacy Talk at Disruptathon, with more than 150 developers*[7]
- *"Check Yourself" Keynote at MoDevEast, with more than 350 developers*[8]
- *"Can Washington Make your App Illegal?" at South by South West (SxSW)*
- *"Best Practices for Privacy Icons" at MoDevUX conference.*
- *"App47 Privacy Webinar" with App47 CEO Chris Schroder*
- *"Talking Privacy with dotnet rocks" : dotnet rocks is a podcast listened to by more than 500,000 developers weekly*
- *"Privacy Bootcamp" at Silicon Valley Apps for Kids Meetup*
- *"Moms with Apps Privacy Icon Working Group"*[9]
- *pii2012 Seattle Bootcamp and Workshop*[10]

In addition, we've frequently brought developers to meetings with lawmakers and regulators here in Washington, including extensive meetings with the White House, FTC, and Members of this Committee as well as dozens of other Members of Congress.

ACT's Approach to Mobile Developers

First and foremost, we advise app developers to be open with consumers about the information they collect and how it is used. We strongly advocate the use of privacy policies – even if an app maker believes no information is being collected. It is also important that this information is presented to users in a meaningful way so that they may easily comprehend it. On mobile devices this means that the information provided must be simple and clear enough to fit on a small screen.

---

[7] http://www.meetup.com/modevdc/events/28701631/

[8] http://vimeo.com/34560160

[9] http://momswithapps.com/privacy-icon/

[10] http://www.privacyidentityinnovation.com/pii2012-seattle/pii2012-seattle-schedule

ACT also advises app developers to be mindful of the relationships they have with third parties such as ad networks. App makers must be aware that the SDKs (software development kits) supplied by platform providers or ad networks may contain code that uses consumer information in ways they hadn't considered. Even if the developer never sees the data which passes straight through to an advertiser, the responsibility still lies with the app maker to inform the user what information is shared and how it is being used. Additionally, developers should ensure that they collect only as much information as is needed. When this information is no longer required, it should be de-identified.

In addition to our own initiatives, other efforts have also been undertaken by industry to provide improved consumer access to privacy information. To address the accessibility of privacy policies, groups like TRUSTe[11] and PrivacyChoice.org[12] provide free privacy policy generators. Developers can simply fill out a survey explaining the functions of their app and a privacy policy is automatically generated. This is a useful option for startups that can't afford legal staff. The resulting privacy policy is generated in both the long form that we are accustomed to seeing (and seldom reading) as well as a more easily digestible version composed of simplified language. The other benefit of these services is that they customize the end product to appear on a small screen.

Moving Forward

Privacy issues must be addressed in a comprehensive manner, not in a way that creates "siloed" solutions for each technology…especially since those silos are disappearing every day.

Everyone in the technology industry must take part and be responsible for improving the state of privacy, security, and transparency across our various industry segments. Our app developer members are no different, and we're committed to working this out with government, industry, civil society, and most importantly, our customers.

That is why we are concerned that approaching these issues based on categories of technology is bound to create incompatibilities, confusion, and customer distrust. We recognize that consumers' confidence in the safety of their privacy is necessary for app makers to effectively market their products. We will continue to work through all the various multi-stakeholder efforts and business-based guideline processes, as well as with the members of this Committee, to improve these efforts.

Thank you for the opportunity to appear before the Committee today and I look forward to addressing any questions you may have.

---

[11] http://www.truste.com/products-and-services/small_medium_business_privacy/privacy_policy_generator.php
[12] http://www.privacychoice.org/resources/policymaker

Mr. GOODLATTE. Mr. Babel, welcome.

TESTIMONY OF CHRIS BABEL,
CHIEF EXECUTIVE OFFICER, TRUSTe

Mr. BABEL. Thank you.

Chairman Goodlatte, Ranking Member Watt and distinguished Members of the Subcommittee, my name is Chris Babel, and I am the Chief Executive Officer of TRUSTe, a leading provider of privacy technology and certification solutions to online companies. Based in San Francisco, TRUSTe offers a suite of privacy solutions to help businesses increase consumer trust and engagement across their Web sites, mobile applications, online advertising and cloud-based services. Over 5,000 companies, such as Apple, AT&T, Disney, eBay and Yelp, rely on TRUSTe to ensure compliance with evolving and complex privacy requirements and to build trust with consumers.

I would like to highlight three topics in my remarks before the Subcommittee today: first, the consumer privacy perspective; second, new privacy challenges and the technologies TRUSTe and others offer to address them; third, why we think that self-regulation has been successful in protecting consumers online.

First, through consumer research we submitted in the written testimony, we know that consumers are concerned about privacy online on both their PC and mobile devices. Take mobile, for example, where 74 percent of consumers believe it is very or extremely important to understand what personal information a mobile application collects. Eighty-five percent want to be able to opt in or opt out of targeted mobile ads. These concerns are causing the consumer to become more engaged in their privacy decisions and more likely to take control of when and how their data is collected and used.

Research also highlighted that 59 percent of consumers generally trust that Web sites are protecting their privacy online, showing that businesses can build trust and alleviate privacy concerns through investments in privacy best practice and privacy technologies.

Second, there is explosive growth in privacy services offered to consumers. In TRUSTe's first 12 years in existence through 2009, we grew it from offering one to four services focused on Web site privacy only. In the past 2½ years we have launched over 10 new services spanning Web sites, mobile applications, online advertising and cloud services.

Taking mobile as an example, since all of you carry mobile devices, the challenges are that less than one-third of mobile applications have a privacy policy today, and when they do, they are difficult to read and need to handle sensitive topics like location information.

TRUSTe offers application providers a free mobile privacy generator, as well as paid services to certify that mobile applications have strong privacy, as well as notice and choice mechanisms for consumers regarding mobile ad targeting.

There have also been entirely new industry efforts, like the Digital Advertising Alliance that have been formed to provide consumers notice and choice around online targeted advertising.

TRUSTe is the largest independent provider of services for the DAA. We have also partnered with the Application Developers Alliance to educate mobile developers on important privacy issues as part of a countrywide educational road show. Technology is evolving more rapidly than ever, and solutions for consumer privacy protection are keeping pace.

Third, self-regulation is a critical component to online privacy, and TRUSTe has helped thousands of companies self-regulate their online privacy for 15 years. Self-regulation is valuable in that it helps companies facilitate global best practices, which simplifies the management and cost of these programs while increasing accountability. Self-regulation can also evolve with technology changes to meet the ongoing needs of consumers. And finally, through safe harbors and due process, self-regulation can provide strong incentives for compliance.

Looking forward, it is clear that consumers are becoming ever more aware of how their personal data is collected and used online, which is important as technology changes, like the decreased cost of bandwidth, computer processing and storage allow for the analysis and use of vast databases of information. Self-regulation provides a flexible privacy protection framework that can quickly adapt to these rapidly changing technologies.

Today, industry has made great progress in self-regulating their privacy practices, and though there is much work to be done, we are confident that the goal of protecting consumers while continuing to innovate will be achieved.

Thank you for the opportunity to testify today. I look forward to your questions.

Mr. GOODLATTE. Thank you, Mr. Babel.

[The prepared statement of Mr. Babel follows:]

Written Testimony of

CHRIS BABEL

Chief Executive Officer

TRUSTe

before the

House Judiciary Committee, Subcommittee on Intellectual Property,
Competition & the Internet

"New Technologies & Innovations in the Mobile & Online Space
and the Implications for Public Policy"

June 19, 2012

Chairman Goodlatte, Ranking Member Watt, and distinguished members of the subcommittee - my name is Chris Babel, and I am the Chief Executive Officer of TRUSTe, a leading provider of privacy technology and certifications to online companies.

Based in San Francisco, California, TRUSTe offers a suite of privacy solutions to help businesses increase customer trust and engagement across all their online channels - including websites, mobile applications, online advertising and cloud services. Over 5,000 companies including Apple, AT&T, Disney, eBay, HP, Microsoft, Nationwide and Yelp rely on TRUSTe to ensure compliance with evolving and complex privacy requirements and build trust with consumers.

TRUSTe was originally founded as a non-profit industry association in 1997. In 2008, we converted to a for-profit company with venture capital investment. This corporate transformation and infusion of resources has allowed TRUSTe to meet evolving privacy challenges head on in the marketplace. In these past four years we have developed robust technology platforms and rapidly expanded the scope and scale of our privacy offerings and certifications. Our products are cost-effective, scalable, and relevant across business models and practices. Consumers, businesses and regulators worldwide recognize the green TRUSTe Privacy Seal, awarded to our clients upon successful certification, as a symbol of strong privacy practices and trust.

TRUSTe's mission, "Truth in Privacy", embodies our overarching goal of bringing greater Transparency, Choice and Accountability to consumers online. We design all of our products and services around these three core principles:

- Transparency – accurate and comprehensive disclosures through the organization's privacy statements and consumer education initiatives
- Choice – mechanisms that allow consumers to proactively set boundaries around the collection and use of their personal information
- Accountability – the ability for consumers to resolve privacy concerns either with the organization directly or through TRUSTe

I would like to highlight three topics in my remarks before the subcommittee today: 1) the consumer's perspective on privacy; 2) new privacy challenges that exist today, and the technologies that TRUSTe and others have developed to address these challenges; and 3) why we think that self-regulation has been successful in protecting consumers online.

The Consumer Perspective

We believe it is critically important to understand consumer privacy perceptions and attitudes when designing privacy frameworks. Toward this end, we have contracted top research firms over the past three years to conduct numerous national surveys to gauge

consumer privacy attitudes and opinions. Key findings that we would like to share with the committee include:

- 90 percent of U.S. adults worry about their privacy online.[1]
- 85 percent of consumers want to be able to opt-in or out of targeted mobile ads.[2]
- Consumer favorability towards targeted advertising doubles if they are assured that personally identifiable information is not used in the process.[3]
- 74 percent of consumers believe it's "very important" or "extremely important" to understand what personal information a mobile app collects.[4]
- 1 in 3 consumers feel that they don't have a choice when it comes to apps collecting their location data.[5]
- Financial information, direct contact information, health information, and current location are the most sensitive categories of information for consumers when it comes to sharing that data with advertisers.[6]

While many of these responses highlight the fact that there is still considerable work to be done, one additional point worth highlighting is that

- 59% of consumers generally trust that most websites protect their privacy online.[7]

What does all of this mean? The research shows that consumers are becoming more engaged in privacy decisions and more likely to take control of when and how their data is collected and used. It also highlights the investments many companies have made to follow privacy best practices and build consumer trust online.

The Privacy Explosion: New Privacy Challenges and Technologies to Address Them

There is no end in sight to the tremendous growth of privacy services. In 2011 TRUSTe completed online privacy certifications for nearly 4,000 companies and successfully resolved over 8,600 consumer complaints (not all were privacy related) through a dispute resolution service we offer free to consumers on behalf of our clients. A copy of our 2011 Transparency Report is provided as an attachment to this testimony and provides further detail on our technology platforms, certification processes and dispute

---

1 http://truste.com/consumer-privacy-index-Q1-2012/
2 http://truste.com/why_TRUSTe_privacy_services/harris-mobile-survey/
3 http://truste.com/ad-privacy/
4 Ibid
5 Ibid
6 Ibid
7 http://www.truste.com/consumer-privacy-index-Q1-2012/

resolution mechanism. Today, I would rather talk about the privacy challenges that lie ahead and the technologies being developed to address them.

The rollout of new technologies and platforms continues at a rapid pace and companies like TRUSTe that offer privacy solutions must move as quickly. The industry shift to mobile devices and the cloud, the growth of online behavioral advertising, and changing global standards have created new privacy challenges, particularly given the underlying reality that data is easier to collect, cheaper to store and faster to analyze (often referred to as "Big Data") than ever before. Let me describe each of these challenges more fully.

Mobile & Wireless Devices

Mobile devices – especially smartphones – present unique privacy challenges because they are carried by many consumers at all times and are in a state of perpetual data collection. There are also challenges around providing consumers with adequate notice and consent mechanisms on a very small screen. We have attempted to meet these challenges in the mobile space in several ways:

- In 2010 TRUSTe launched the industry's first mobile app privacy certification program, leveraging technology to verify app data collection and requiring extra privacy protections around sensitive data collections like user location data. That same year we also introduced an innovative privacy policy format for mobile devices that makes privacy policies readable and user-friendly on mobile devices (see Figures 1 & 2 on next page).

- In 2011 TRUSTe released a free online privacy policy generator leveraging this mobile format, allowing app developers nationwide to create policies for their apps and mobile websites.

- In 2012 we partnered with the Application Developers Alliance to educate mobile developers on important privacy issues as part of a countrywide educational roadshow. This year, we also launched TRUSTed Mobile Ads, a pioneering technology platform that notifies consumers of advertising tracking on their mobile devices and enables them to opt-out if they desire.

Figure 1 –
TRUSTe Mobile Privacy Policy

Figure 2 –
Tracking & Ads Disclosure Section

Cloud

Software is increasingly imbedded in all aspects of daily life. With the increases in bandwidth and connectivity over the past decade, software has transitioned from being managed on premise to being managed in the cloud, often times at locations that are unknown to the end customer. These cloud services are used for everything from backing up consumers' computer files to housing the corporate records and financial statements of some of the largest companies in the world.

To address the privacy challenges of cloud services, TRUSTe added new certification programs to help consumer or business customers understand the data collection, storage and use practices of these cloud service providers.

Online Behavioral Advertising

The sheer scope and complexity of online tracking and advertising given the rise of "Big Data" have created daunting privacy challenges. Consumers have historically been under educated regarding targeted advertising and did not have meaningful control over their data. Industry has banded together to form an organization called the Digital

Advertising Alliance (DAA). This effort, spearheaded by the American Association of Advertising Agencies, the American Advertising Federation, the Association of National Advertisers, the Better Business Bureau, the Direct Marketing Association and the Interactive Advertising Bureau has developed www.aboutads.info to educate consumers and give them control over targeted ads.

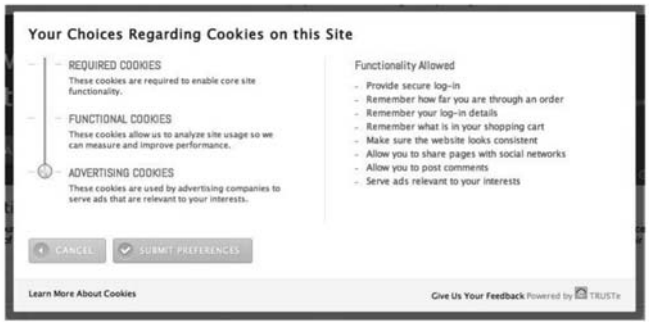
TRUSTe is a service provider for this industry effort. Our TRUSTed Ads program is a technology platform that provides consumers with privacy notice and opt-out choice for targeted advertising on webpages and display ads where tracking occurs. Today we are the largest independent provider of compliance technology for the DAA program.

Changing Global Standards

Privacy has become a global issue and other countries have adopted different frameworks and regulations. For instance, TRUSTe has kept a close eye on data protection developments in the EU. As an EU Safe Harbor Provider since 2001, we have helped many clients comply with the EU's unique data protection requirements around data transfers. Earlier this year, we began delivering privacy solutions to provide users choice and notice under the EU's new "Cookie Laws" which regulate online tracking and targeted advertising.

These solutions include our EU Cookie Audit, a powerful auditing technology that can detect and report on all first and third-party tracking mechanisms present on a website. Our clients operating in the EU have used this auditing technology to gain key insight into the scope of data collection on their properties and to prepare for compliance with EU privacy laws. These clients then use our TRUSTed Consent Manager (see Figure 3) on their sites to allow consumers to express or withdraw their consent to be tracked. The Consent Manager can be implemented based on the specific requirements of each EU Member State's Cookie Law.

Figure 3 – TRUSTed EU Consent Manager



Self Regulation Works

TRUSTe has helped thousands of companies self-regulate their online privacy practices for 15 years and this experience has reinforced our belief that self-regulation is a critical component to any privacy framework. We think that there are at least 3 reasons why self regulation works when it comes to online privacy and data protection:

Self-Regulation Facilitates Global Best Practices. Self-regulatory programs like those offered by TRUSTe can integrate national and international privacy frameworks into a unified program that allows companies to satisfy regulatory requirements and best practices from around the globe. The advantages of making a set of unified changes, instead of continually re-adjusting them for each market and jurisdiction cannot be overstated and create a powerful incentive for companies to self-regulate to higher standards than might be required in any one jurisdiction.

Self-Regulation Can Evolve With Technology – Online privacy frameworks must be dynamic, like the technology they regulate. At TRUSTe, we are constantly adding and updating our program requirements to keep pace with the fascinating and rapidly changing technologies we are seeing in the marketplace. We remain committed to recommending privacy standards that evolve with technology and that are appropriate – not just to the context, but also the privacy expectations of the transaction. This contextual approach helps us adapt our frameworks quickly in response to emerging online and mobile services.

Self-Regulation Can Provide Strong Incentives for Compliance – Self-regulation can encourage compliance by industry through participation incentives. Two important incentives include:

- **Safe harbors** to help foster the growth and promotion of best practices, which in turn are critical to the overall success of a self-regulatory framework.

- **Due Process** to preserve incentives for companies to certify and self-regulate their privacy practices within voluntary frameworks. Under TRUSTe's certification process, due process includes appropriate confidentiality and adequate procedural safeguards, and the opportunity to cure a mistake.

Conclusion - Looking Ahead

As the leading provider of privacy technology and certifications to online companies TRUSTe has had unique insights into the technology changes driving the online ecosystem and their privacy impacts. Looking ahead we see three major trends that will impact future privacy frameworks:

- **The Engaged Consumer** – It is clear that consumers are becoming ever more aware of how their personal data is collected and used online. Mainstream press coverage on privacy has increased significantly in the past few years and consumers have become better informed and proactive about protecting their privacy across devices and platforms. The availability of usable privacy tools and meaningful privacy disclosures will become even more important as this trend continues.

- **Big Data** – Today's companies are racing ahead to harness the aggregate power of vast databases of personal data.[8] Personal data is a critical asset for businesses and leveraging that data can yield tangible benefits for both business and consumers. For example, by leveraging its clinical and cost data, Kaiser Permanente was able to attribute 27,000 deaths to Vioxx and pull the drug off the market.[9] As companies accelerate their use of "Big Data" we see technology playing a much larger role in protecting user privacy in online ecosystems.

- **The Rise Towards Accountability** - Consumers, industry groups and international bodies are all calling for frameworks that hold industry participants accountable to the promises they make to consumers and the standards they voluntarily adopt – regardless of the platform or device that is being used.

For these reasons, TRUSTe believes in self-regulation as a critical component in addressing online privacy challenges. Self-regulation provides a flexible privacy protection framework that can quickly adapt to rapidly evolving technologies. Industry has made great progress on self-regulating their privacy practices, and though there is still much work to be done, we are confident that the goal of protecting consumers - while continuing to innovate – will be achieved.

Thank you for the opportunity to testify today. I look forward to your questions.

---

[8] Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 Stan. L. Re. Online 63 (2012).
[9] Id at 64.

ATTACHMENT

TRUSTe TRANSPARENCY REPORT: **2011**

TRUSTe Inc.
835 Market Street
Suite 800
San Francisco, CA 94103
888.878.7830
www.truste.com

Contents

Introduction 3

2011: Year in Review 4

TRUSTe Privacy Program Requirements 4

The TRUSTe Approach 5

Certification 5

Compliance 6

TRUSTed Websites and TRUSTed Websites Basic 6

EU Safe Harbor 7

TRUSTed Cloud Certification 8

TRUSTe Mobile Site and App Certification 8

TRUSTed Data Collection 8

TRUSTed Ads 8

TRUSTe Consumer Dispute Resolution 9

Enforcement 9

TRUSTe Research 11

Looking Ahead in 2012 11

Appendix A: TRUSTe Privacy Certification Programs – Growth & Participation 13

Appendix B: TRUSTe's Privacy Program Requirements 14

Appendix C: TRUSTe's Enforcement Summary – (2009-2011) 15

Appendix D: TRUSTe Consumer Dispute Resolution Data 16

1. Consumer Dispute Resolution Volume (2007-2011) 16

2. Consumer Complaints Organized by Outcome (2011) 16

3. Consumer Complaints Organized by Type (2011) 18

Appendix E: Consumer Dispute Resolution Process 19

2011 Consumer Survey Responses re: TRUSTe's Consumer Dispute Resolution Mechanism . . . 19

Introduction

TRUSTe has helped companies build consumer trust and achieve online privacy compliance since 1997.[1] As the leading provider of online privacy management solutions, we certify clients of all sizes — with certification options that are cost-effective, scalable, and relevant across business models and practices. The TRUSTe seal is recognized globally by consumers, businesses and regulators as a symbol of online privacy compliance.[2]

TRUSTe's core mission is *Truth in Privacy*[3] — a philosophy embodied by our Privacy Program Requirements which are built on three important privacy principles — **Transparency**, **Choice** and **Accountability**. When consumers see the TRUSTe Seal, they can be confident that the organization provides:

- **Transparency** – accurate and comprehensive disclosures through the organization's privacy statements and consumer education initiatives.
- **Choice** – mechanisms that allow consumers to proactively set boundaries around the collection and use of their personal information.
- **Accountability** – the ability for consumers to resolve privacy concerns either with the organization directly or through TRUSTe.

In 2011, TRUSTe made important updates to our privacy program requirements, while launching new privacy management solutions for cloud services, mobile sites/apps, and online behavioral advertising. In the spirit of *Truth in Privacy*, we are pleased to issue the TRUSTe Transparency Report — detailing all of these 2011 developments, while also providing an overview of our certification, consumer dispute resolution and enforcement processes. The appendices provide additional data on TRUSTe's certification programs, and details on consumer complaints received and processed through our dispute resolution service.

The TRUSTe Transparency Report will be issued on an annual basis. We hope you find this information helpful in understanding more about TRUSTe, and our commitment to *Truth in Privacy*.

Sincerely,

Chris Babel, CEO

[1] Based in San Francisco, California, we were founded as a non-profit, industry association. We converted to for-profit status, with venture investment, in 2008.

[2] TRUSTe has been a EU Safe Harbor Privacy Provider for independent validation and dispute resolution since 2000. Since 2001, we have also served as an an FTC-authorized safe harbor under the Children's Online Privacy Protection Act ("COPPA").

[3] To learn more about the TRUSTe's *Truth in Privacy* Mission, visit: http://www.truste.com/about_TRUSTe/

2011: Year in Review

In 2011, TRUSTe completed privacy certifications for over 4,000 companies representing approximately 7,000 separate URLs (covering a range of websites, cloud services, mobile apps, etc.). Also in 2011, TRUSTe's Consumer Dispute Resolution Service processed over 8,500 consumer complaints.

Building on the foundation of our Website Privacy Certification program, which includes support for COPPA, EU Safe Harbor and mobile privacy, TRUSTe launched two new certifications in 2011 — TRUSTed Cloud and TRUSTed Data Collection. In addition, TRUSTe became a DAA-approved provider for online behavioral advertising ("OBA") compliance in the United States with our TRUSTed Ads product.

A table illustrating TRUSTe's 2011 certification and compliance products is provided below:

TRUSTe Product	Program Basis	Intro and Last Update
TRUSTe Website Certification including EU Safe Harbor & Mobile **TRUSTed Websites: Enterprise/Higher Risk** **TRUSTed Websites Basic: Small & Medium/Lower Risk**	OECD Guidelines, FTC Fair Information Practices, US – EU Safe Harbor Principles, other regulatory and industry guidelines such as CAN SPAM, CTIA, emerging mobile privacy best practices	Launched 1997 Last Update 2011
Children's Online Privacy Certification	FTC Fair Information Practices + COPPA Rule	Launched 2001 Next update 2012
TRUSTed Cloud	US – EU Safe Harbor Framework, CSA Guidelines, other regulatory and industry guidelines, and emerging practices	Launched March 2011
TRUSTed Data Certification	TRUSTed Data Certification	Launched May 2011
TRUSTed Download	FTC Fair Information Practice Principles, industry guidelines and evolving best practices	Launched 2005
TRUSTed Ads	US Digital Advertising Alliance; Advertising Industry Guidelines	Launched January 2011

TRUSTe Privacy Program Requirements

TRUSTe's Privacy Program Requirements form the basis upon which we certify the privacy practices of our clients. TRUSTe's Privacy Program Requirements are referenced in Appendix B to this report and is also posted online.[4]

TRUSTe's Privacy Program Requirements incorporate the principles of Notice, Choice, Access, Security and Enforcement — as reflected in (i) the Department of Commerce's Consumer Privacy Bill of Rights, (ii) the privacy frameworks established by Asia Pacific Economic Cooperation ("APEC") and the Organization for Economic Cooperation & Development ("OECD"), (iii) regulatory guidance from the Federal Trade Commission ("FTC"), and (iv) regulatory guidance from other jurisdictions, including the EU. They also reflect (i) input from consumers, (ii) TRUSTe clients, (iii) consumer protection advocates, and (iv) business trade associations.

[4] TRUSTe's Privacy Program Requirements are available at: http://www.truste.com/privacy-program-requirements/home

The following are examples of what TRUSTe considers a material change:

- Changes to a client's practices regarding notice, collection, use, and disclosure of PII and/or Third Party Personally Identifiable Information;
- Changes to a client's practices regarding user choice and consent to how PII, and/or Third Party PII, is used and shared; or
- Changes to a client's measures addressing information security, integrity, access, or individual redress.

TRUSTe's Privacy Program Requirements cover the collection and use of personally identifiable information or "PII." Under our Privacy Program Requirements, PII is defined as "any information or combination of information that can be used to identify, contact, or locate a discrete Individual." We believe that companies need to be transparent about their data collection practices — because discrete data elements (while lacking identifying characteristics on their own) can be used in combination to personally identify consumers.[5]

TRUSTe's Privacy Program Requirements take into account the context of a business practice — specifically, what type of data is being collected, for what purpose, and with whom is it being shared — before imposing appropriate privacy obligations for that practice. For example, our requirements around notice and consent vary depending on what type of PII is being collected and how it is being used. Under TRUSTe's Privacy Program Requirements, notice and express consent is required for all sharing of PII that we define as "sensitive" (e.g. financial, medical and geo-location data). For non-sensitive PII, TRUSTe requires notice and inferred consent.

TRUSTe's Privacy Program Requirements also address certain "material changes" in a client's privacy practices, which we define as the "degradation in the rights or obligations regarding the collection, use, or disclosure of PII for an Individual." All clients are contractually bound to notify TRUSTe of any such a material change in their privacy policy/practices. In addition, we consider changes that involve PII collection, use, or disclosure as material; clients must notify users prior to making such a change.

The TRUSTe Approach

Certification

TRUSTe's approach to website privacy certification can differ based on the complexity of the client's business and privacy practices. TRUSTe works with clients of all sizes to provide cost-effective, scalable, privacy solutions that work across different types of business models. In this way, we aim to promote strong privacy practices across the online ecosystem.

TRUSTe's oversight of a client's privacy practices begins with the initial contact, and spans the entire client relationship. Even before a new client is signed, our sales team is trained to recognize potential issues that might trigger additional obligations (e.g. additional requirements around the collection of personal data from children, that will require COPPA certification).

All TRUSTe privacy certifications begin with a risk assessment of the client's business and privacy practices, which can differ, depending on the client's business model, and the features and functions of the client's website, app, or online service. The goal of the risk assessment and review process is to ensure that the client is ready for TRUSTe Certification — and this can only happen when the client's stated practices and actual practices match up to TRUSTe's Privacy Program Requirements. We then determine which TRUSTe certification best matches the client's needs.

TRUSTe uses a combination of three different methodologies to conduct the privacy certification review: a manual evaluation of the client's practices, the client's own attestations and interviews, and monitoring through TRUSTe's proprietary technology and tools. The extent to which we use one methodology over another is dependent on a client's risk profile. We examine how the client collects, uses and shares personal data; we also identify the client's third party, data-sharing relationships.

[5] This is a forward thinking perspective that was advanced by FTC staff in a recent online privacy report. Specifically, staff noted "the blurring of the distinction between personally identifiable information and supposedly anonymous or de-identified information. FTC Staff Report, Protecting Consumer Privacy in an Era of Rapid Change (2010), available at: http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

TRUSTe privacy certification is backed by one of our strongest assets: the TRUSTe certification team. Certification team members are selected for their substantive knowledge of relevant privacy and technology issues[6], as well as their hands-on experience in evaluating privacy concerns from clients representing a broad spectrum of online business models. The certification team performs and analyzes initial certifications, conducts post-implementation checks (once the client installs the TRUSTe seal and posts the TRUSTe-certified privacy policy), and manages the re-certification process.

Nearly all clients must make changes to their existing practices or privacy policy to qualify for TRUSTe certification. In some cases making changes to existing practices simply isn't enough: in 2011, 9% of applicants for TRUSTed Websites and TRUSTed Websites Basic certification did not complete the process because they were unable or unwilling to make the changes required under the TRUSTe Privacy Program Requirements. This represents a smaller number than in 2010 — when 12% of applicants didn't make the changes required, and were therefore not eligible for TRUSTe certification.

TRUSTe charges companies for privacy management solutions based on a number of factors: the size of the organization (either measured by revenue or pages served), the complexity of the client's business model and privacy practices (we charge more, for example, if there are a number of different brands with different websites under one company), the volume of personal data collected, and the number of TRUSTe solutions purchased. TRUSTe also retains the option to decline or terminate certification in situations where we cannot certify an applicant's business model, or where the applicant's business model is otherwise sufficiently problematic to warrant denial (e.g. an application or website involving online gambling).

Compliance

Once a client completes the initial certification process, TRUSTe uses a combination of approaches to ensure that compliance with TRUSTe's Privacy Program Requirements is consistently and continually maintained. Unlike an audit — which only captures compliance at a single point in time — TRUSTe certification involves ongoing monitoring using a combination of inquiries/reviews and technological tools. These tools include:

- **Web crawling**: Proprietary TRUSTe technology that verifies the existence of key website elements (e.g. a privacy policy at the point of PII collection), and website processes (e.g. the transmission of credit cards and other sensitive information over an encrypted connection). TRUSTe's web crawler also performs intensive website analysis for data collection and ad targeting processes, and in conjunction with other techniques serves as TRUSTe's technological accountability platform for monitoring clients.
- **E-mail seeding**: A process by which compliance is monitored using unique e-mail addresses that do not reference TRUSTe, to check for e-mail sent by an unauthorized party, or after an unsubscribe request has been processed.[7]
- **Traffic analysis**: A network packet monitoring process primarily used to verify compliance for our mobile privacy and Trusted Download certifications.

At least once a year, TRUSTe investigates whether its clients are meeting and/or exceeding TRUSTe's Program Requirements through a re-certification process. If the client notifies TRUSTe of a change or TRUSTe detects a change outside the 'annual' re-certification cycle, the change will be verified by TRUSTe immediately, regardless of whether it's time for the client's annual re-certification or not.

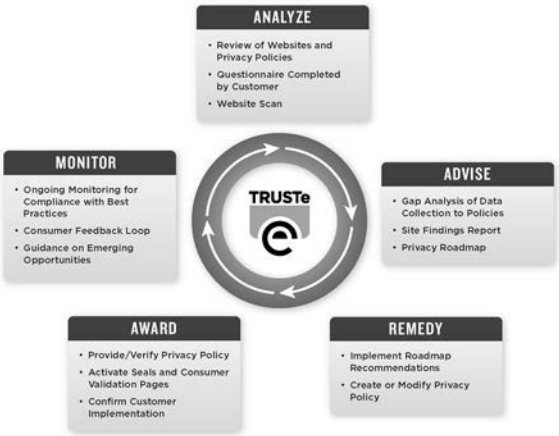
TRUSTed Websites and TRUSTed Websites Basic

The first step in our web privacy certification process is to determine whether the client has unique business needs that require TRUSTed Websites, our more customized privacy solution, or whether the client's privacy needs can be met through TRUSTed Websites Basic, our semi-automated solution. Both solutions — TRUSTed Websites and TRUSTed Websites Basic — are based on the same set of comprehensive TRUSTe Privacy Program Requirements, and are represented by the same TRUSTe seal.

[6] Most members of the TRUSTe certification team have a CIPP certification, (with some of the team having a J.D. or M.B.A. degree), in addition to prior, relevant, job experience (e.g. audit, paralegal). TRUSTe encourages all certification team members to become CIPP certified. New certification team members get a comprehensive orientation on privacy law and policy, prior to engaging with clients. This is supplemented by continuing, extensive, on-the-job training on important changes to global privacy laws, policy and regulations.

[7] TRUSTe's e-mail seeding process has had notable successes in cases where the client or seal holder was not initially aware of an unsubscribe malfunction or data leakage (through a service provider, for example). In such cases, TRUSTe's e-mail seeding report has alerted clients to the issue, and supported TRUSTe's recommendations for issue resolution.

The TRUSTed Websites certification process involves five steps: analyze, advise, remedy, award and monitor. The diagram below illustrates the specifics of this approach:



For small and medium sized clients with low-risk business practices, our TRUSTed Websites Basic is often the right solution. TRUSTed Websites Basic was primarily designed for small and medium-sized businesses in mind. In our experience however, we have found that privacy risk does not always correlate to company size; a very small business can have incredibly complex data collection and management practices, while very large companies can sometimes have very simple data collection and use practices.

TRUSTed Websites Basic features our automated Privacy Policy Generator — an innovative TRUSTe technology that certifies businesses against TRUSTe's Privacy Program Requirements while providing a cost-effective privacy solution. TRUSTe's Privacy Policy Generator scans a prospective client's website and based on this information and other client input, generates a privacy policy that is hosted by TRUSTe. TRUSTed Websites Basic is backed by all of the features that strengthen TRUSTe's custom privacy certification — clients must contractually agree to abide by the TRUSTe-generated privacy policy and submit to our consumer dispute resolution process.

More details on TRUSTe's Website Privacy Solutions are at: http://www.truste.com/website-privacy

EU Safe Harbor

TRUSTe has helped companies prepare for self-certification under the US-EU and US-Swiss Safe Harbor Frameworks — administered by the Department of Commerce — since 2001. We also provide the independent third party dispute resolution mechanism, required under these frameworks, to address consumer complaints.

TRUSTe's Privacy Certification Program Requirements are based in large part on current EU data protection requirements. We require that clients only use data for purposes that were stated at the time of collection, and provide choice for secondary uses that were not agreed to at the time of collection. Consumers have the right to request access to their PII for the purpose of updating, correcting, or deleting it. Finally, TRUSTe requires that all EU Safe Harbor clients add a statement to their privacy policies regarding their compliance with the US-EU/Swiss Safe Harbor Frameworks.

More details on how TRUSTe can help you comply with the EU-US Safe Harbor framework are at: http://www.truste.com/eu-safe-harbor

TRUSTed Cloud Certification

TRUSTe launched its TRUSTed Cloud certification in March 2011. This program certifies the privacy practices of "Service Providers" — companies that process data on behalf of another entity. TRUSTe reviews and assesses the privacy practices of data collected through the Service Provider's platform or service portal focusing on how the Service Provider manages and processes the data collected on behalf of its clients. Areas of assessment include: collection limitation and use; and data management processes such as sub-processor vetting, security, and data retention policies.

More details on TRUSTe's Cloud Privacy Solutions is at: http://www.truste.com/cloud

TRUSTe Mobile Site and App Certification

TRUSTe's Mobile certification program was launched in November 2010 and provides certification for both mobile applications and mobile-optimized websites.

A particular focus of our mobile certification program is the collection and use of precise geo-location data and device identifiers. TRUSTe classifies "precise geo-location data" as sensitive data that requires the user's express consent prior to collection and use. We also require clients certified under this program to provide a short notice privacy statement, optimized for navigation and viewing on a mobile device. The privacy notice must include disclosures around whether precise geo-location data is collected, and what types of tracking may occur. As part of the mobile (app) certification, TRUSTe's evaluates permissions that the application is granted, what data is gathered, and with whom it is shared.

More details on TRUSTe's Mobile Privacy Solutions is at: http://www.truste.com/mobile

TRUSTed Data Collection

The TRUSTed Data Collection certification program was launched in May 2011 to address the data collection and use practices of companies that collect data across multiple unaffiliated websites over time. These companies are known as third party data collectors – they collect data through websites or applications they do not own. By way of example, these types of companies would include ad networks, data aggregators, analytics companies, and demand side platforms [DSPs].

The key components of TRUSTed Data Collection certification are: understanding the types of data collection (including the types of technologies used), what type of data is collected both directly and from third party sources, how that data is used, and how consumers are able to exercise choice over the use of that data. Third party data collectors must obtain the consumer's express consent prior to collecting PII, or prior to using sensitive data such as health information for targeted marketing. Collection of data from children under age 13 is not allowed under this program.

More details on TRUSTed Data Collection is at: http://www.truste.com/data

TRUSTed Ads

In 2011, TRUSTe became a DAA-approved Online Behavioral Advertising (OBA) compliance provider with its TRUSTed Ads program. TRUSTed Ads allows companies across the online advertising ecosystem — advertisers, publishers, agencies, and networks / platforms — to achieve reliable, scalable, and cost-effective compliance with the DAA's Self-Regulatory Program.

As of December 2011, TRUSTe had served the DAA icon on well over 100 billion ad impressions.

More details on TRUSTed Ads is at: http://www.truste.com/ads

TRUSTe Consumer Dispute Resolution

Consumer dispute resolution is a key component of TRUSTe's privacy management solution suite and helps us monitor client compliance and keep them accountable for their privacy practices. Processing consumer disputes also provides TRUSTe with a window into the privacy issues that concern today's online consumers. We have provided excerpts from our 2011 consumer dispute resolution survey in Appendix E to this report.

The TRUSTe Consumer Dispute Resolution process begins with a consumer complaint filed against a TRUSTe client either with the company, or with TRUSTe. After TRUSTe receives a complaint, we initiate an investigation. A TRUSTe investigation may also be initiated after a TRUSTe scan, a media report, regulator inquiry or information obtained through other credible sources.

Once TRUSTe has reviewed the complaint, the consumer receives TRUSTe's initial response within 10 business days, our published time frame. The nature and duration of the investigation needed can vary widely depending on the nature of the issue. TRUSTe quickly checks all issues that can be immediately verified. If our findings do not verify what the consumer alleged, we inform the consumer at the time. If we need more information from the client, we request it. The client ordinarily has 10 business days to provide a written response for the consumer. For more urgent issues, such as security vulnerabilities, we escalate to the client via phone as well and generally expect responses much sooner, especially if we are able to verify the problem.

Enforcement

TRUSTe certification is fortified by strong enforcement of our privacy program requirements and our consumer dispute resolution process. Because TRUSTe privacy certification is completely voluntary, our challenge is to preserve the incentives for companies to certify and self-regulate their privacy practices within a voluntary framework, while also remaining true to our *Truth in Privacy* mission. Part of addressing that challenge is to ensure that appropriate confidentiality and adequate procedural safeguards, including the opportunity to cure, are part of the enforcement process.

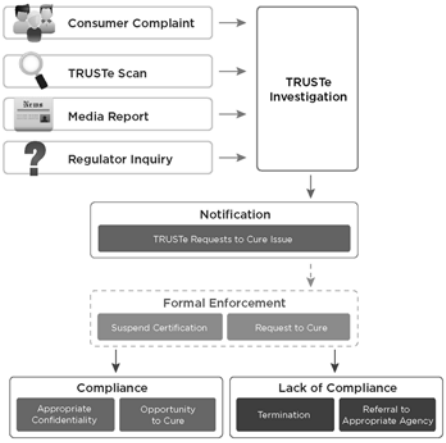
The TRUSTe enforcement process usually begins with an internal compliance investigation. TRUSTe may initiate this investigation based on results of our technological monitoring, on information contained in a consumer complaint, news or press reports, regulator inquiry, or reports from other credible sources.

Our investigations have one of three possible outcomes:

- An agreement between TRUSTe and the client over the privacy complaint — resulting in client resolution that addresses the consumer concern or request.
- A disagreement — triggers a notice of formal enforcement, resulting in the client's suspension or notice of intent to terminate for cause if the matter is not cured.
- A failure to implement the required cure — results in the client's termination from TRUSTe's program and, in extreme cases, publication and/or referral to an appropriate authority.[8]

[8] One of our prior FTC referrals was ClassicCloseouts in 2008; TRUSTe assisted the FTC with the investigation, and the agency brought action for permanent injunction and relief against the site, ultimately obtaining a $2.08 million settlement to provide redress for consumers. See Merchandiser Who Illegally Charged Consumers' Accounts Settles with FTC, available at: http://www.ftc.gov/opa/2011/01/classicclose.shtm.

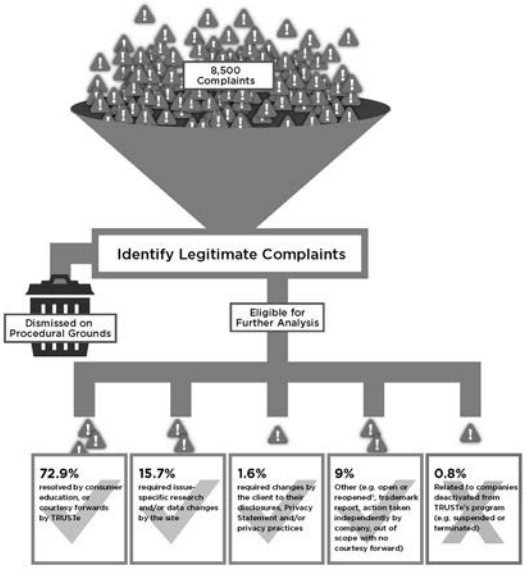
The diagram below illustrates TRUSTe's consumer dispute resolution and enforcement processes:



In 2011, TRUSTe handled over 8,500 complaints, most of which were from consumers. The majority of complaints were resolved before any formal enforcement procedure (under our certification programs) was needed. In addition, nearly half of all consumer complaints were closed on procedural grounds — e.g. nonsensical typing, invalid email address, consumer did not give permission for TRUSTe to pass identifying information to the site (such as needed for investigating and responding to account-specific issues).

Of the remaining 2011 complaints:

- 72.9% were resolved by consumer education, or courtesy forwards by TRUSTe (such as for transactional or non-privacy issues)
- 15.7% required issue-specific research and/or data changes by the site (e.g. unsubscribe the user, close the account, remove unauthorized profile)
- 1.6% required changes by the client to their disclosures, Privacy Statement and/or privacy practices (including duplicate complaints by different consumers about the same underlying issue)



Additional details on consumer complaints are available in Appendix D.

These statistics demonstrate that in those instances where there is a valid consumer complaint, TRUSTe clients will address an identified problem with the appropriate measure needed to protect their marketplace reputation, and to preserve consumer good will. Often, TRUSTe works hand-in hand with clients to develop the right solution, without penalizing the client for non-compliance. As a result, clients are incentivized towards better privacy practices. By working with clients to quickly address the problem, we also reduced the number of formal enforcement actions that we needed to pursue in 2011 (for more details on enforcement actions, see Appendix C).

[9] 0.6% open or reopened

TRUSTe Research

In addition to certification, TRUSTe provides consumers and businesses with important information and research about key privacy trends. In 2011, we published a series of privacy research studies that focused on the consumer experience including:

- 2011 Mobile Privacy Study (March 2011):
  http://www.truste.com/why_TRUSTe_privacy_services/harris-mobile-survey/TRUSTe-Consumer-Mobile-Privacy-Insights-Report.pdf
- 2011 Online Behavioral Advertising Study (July 2011):
  http://www.truste.com/ad-privacy
- 2011 TRUSTe Privacy Index: Website Edition (November 2011):
  http://www.truste.com/privacy-index-2011-websites

We conducted the two privacy studies in partnership with Harris Interactive. Our Mobile Privacy Research found that privacy was the number one concern for smartphone users when operating their devices. 85% of respondents also indicated that they want the choice to be able to opt-in or out of targeted mobile advertisements, showing strong consumer support for an extension of the DAA self-regulatory to the mobile platform. Our Behavioral Advertising research found that consumers react more positively toward online advertisers who are compliant with the DAA self-regulatory program for behavioral advertising and also found that 37% felt uncomfortable with targeted online advertisements based on their browsing behavior or personal information.

The TRUSTe Privacy Index: 2011 Website Edition was the inaugural release of an ongoing Privacy Index series we will release. The 2011 Website Edition analyzed the privacy disclosures of the top 100 websites in the U.S. and found that on average these policies required a reading level of a college sophomore, where the average U.S. reading level is that of eighth grader. Moreover, at 2,464 words, the average privacy policy is nearly twice the length of the Declaration of Independence. We also found that only 2% of the policies analyzed were optimized for viewing on a mobile device, demonstrating a strong need for privacy policy innovation to adapt to a growing mobile audience.

Looking Ahead in 2012

In 2011 TRUSTe observed dynamic changes in the online data ecosystem that will continue to challenge online privacy compliance in 2012. Three important technological shifts — the migration from desktop to the cloud, the explosive growth of mobile apps, and the increased prevalence of social networking — will continue to revolutionize the way consumers communicate and share information.

In 2012, TRUSTe will continue to work with our clients — so they remain accountable in their data collection practices even as they continue to incorporate new technology into their products and services. Our newer certification programs launched in 2011 — TRUSTed Cloud and TRUSTed Data Collection — will provide us with an even deeper look into the privacy issues that concern businesses and consumers today. As a result, we expect further updates to our Program Requirements and certification processes in 2012.

We are also streamlining our consumer dispute resolution processes to improve the overall user experience, reduce unrelated complaints, and generate improved user feedback. Of course, we continue to train our certification and sales teams on relevant updates to global privacy law, regulation and practice.

TRUSTe sees a strong role for educating consumers and businesses about good privacy habits in 2012. Consumers are becoming aware of privacy issues outside of the "identity theft" arena, with increased concern around tracking and targeting for online advertising, the unauthorized aggregation of personal data in individual profiles, and mobile privacy. Businesses continue to look for answers, as they evaluate new and important business opportunities on the desktop and mobile web. Education is a key piece of the compliance puzzle — particularly as data protection regulators around the world have stepped up investigations and enforcement of personal data collection and privacy practices, a trend that we think will continue to grow in 2012 and beyond.

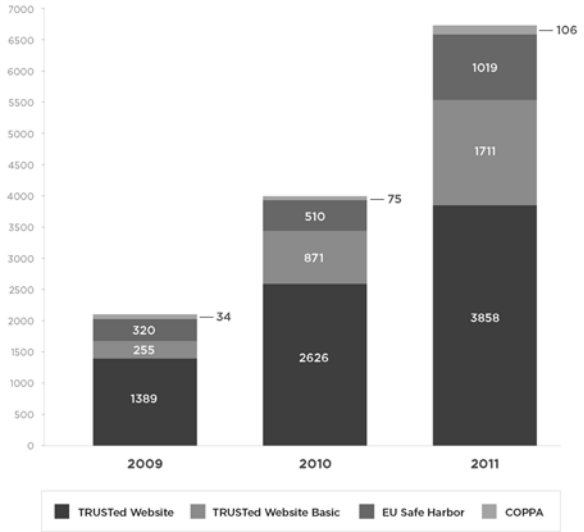
Finally, we see increased scrutiny of self-regulation in 2012 and beyond. While public attention continues to focus on data protection, the role of self-regulatory or accountability programs — like TRUSTe's voluntary, privacy certification programs — has been elevated. Indeed, the rapid changes in technology during the past few years have further reinforced for TRUSTe the importance of self-regulation when developing a framework to protect consumer data. A self-regulatory model, if articulated correctly, is best equipped to deal with complex industries and technologies in a way that preserves incentives for all players involved. Increasingly, as the TRUSTe brand and privacy-related service offerings help businesses address today's privacy challenges and build online trust with consumers, we see a robust future market for privacy solutions that are based on self-regulatory frameworks. This is evidenced by TRUSTe's own growth — participation in our certification programs grew by over 60% in 2011.

In a market economy, self-regulation is driven by a company's desire to advance trust in their brand through exemplary privacy practices. That's why TRUSTe works closely with our clients, helping them launch new products and services while incorporating requirements from updated privacy laws and regulations, into existing privacy compliance programs. This is perhaps the strongest value proposition for any company considering TRUSTe certification. At a time when privacy compliance standards remain in flux, TRUSTe gives companies the confidence to deploy new products and services — by providing them with a data protection framework that is both agile and relevant to today's online business.

APPENDIX – A

TRUSTe Privacy Certification Programs – Growth & Participation

The following chart illustrates the growth in the following certification programs from 2009 – 2011: TRUSTed Websites and TRUSTed Websites Basic, COPPA, and EU Safe Harbor privacy certification programs.



APPENDIX – B

TRUSTe's Privacy Program Requirements

Privacy Certification
http://www.truste.com/privacy-program-requirements/program-requirements

Website Privacy*
http://www.truste.com/privacy-program-requirements/program_requirements_website_privacy

Mobile App/Website Privacy*
http://www.truste.com/privacy-program-requirements/program_requirements_mobile_privacy

Email Privacy*
http://www.truste.com/privacy-program-requirements/program_requirements_email_privacy

EU Safe Harbor*
http://www.truste.com/privacy-program-requirements/program_requirements_EUSH_privacy

TRUSTed Cloud
http://www.truste.com/privacy-program-requirements/trusted-cloud

TRUSTed Data Collection
http://www.truste.com/privacy-program-requirements/3rd-party-data-collection

TRUSTed Download
http://www.truste.com/pdf/Trusted_Download_Program_Requirements_Website.pdf

Children's Privacy
http://www.truste.com/pdf/Childrens_Privacy_Seal_Program_Requirements_Website.pdf

*These certification are modules to TRUSTe's Privacy Certification Program Requirements for clients who seek certification for specific online data collection practices.

APPENDIX – C

TRUSTe's Enforcement Summary – (2009–2011)

Year	Formal Enforcement Actions	Outcome
2009	7 enforcement actions	4 resulted in termination for cause, and 3 additional Suspensions were cured.
2010	3 enforcement actions	2 resulted in terminations for cause; the third involved a Suspension that turned into termination for cause in 2011.
2011	11 enforcement actions	10 resulted in terminations for cause, the third involved a Suspension that was cured.

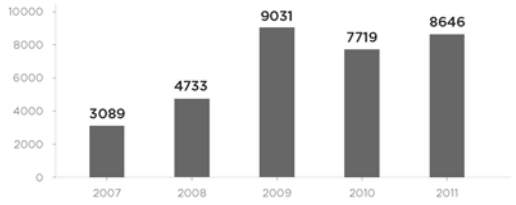
APPENDIX – D

TRUSTe Consumer Dispute Resolution Activity

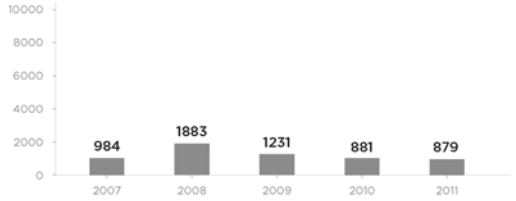
1. Consumer Dispute Resolution Volume (2007-2011)

The following charts summarize volume changes in consumer complaints received by TRUSTe's Dispute Resolution program from 2007 – 2011:

Overall



EU

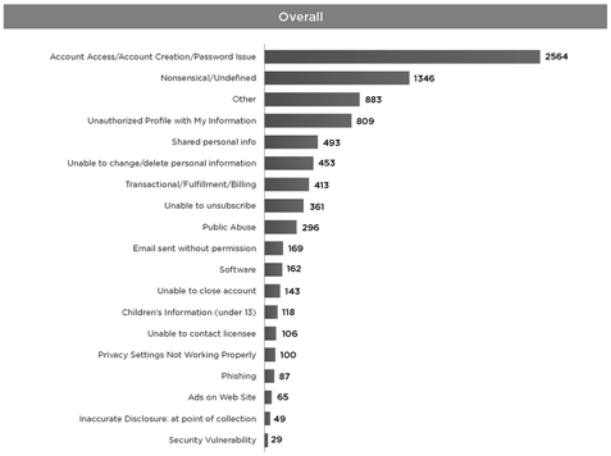


2. Consumer Complaints Organized by Type (2011)

TRUSTe categorizes consumer complaints by the type of complaint filed. When filing a complaint, consumers self-select the category for their complaint based on options provided via a pull-down menu. In situations where TRUSTe does not receive additional information that clearly indicates that a different category is more appropriate, we generally leave the category as the consumer identified it.

While TRUSTe tracks the number of consumer complaints received, many complaints turn out to be requests for service assistance from the client, are nonsensical, or do not otherwise indicate a violation of TRUSTe's Privacy Program Requirements.

The following charts show the types of consumer complaints received by TRUSTe in 2011:



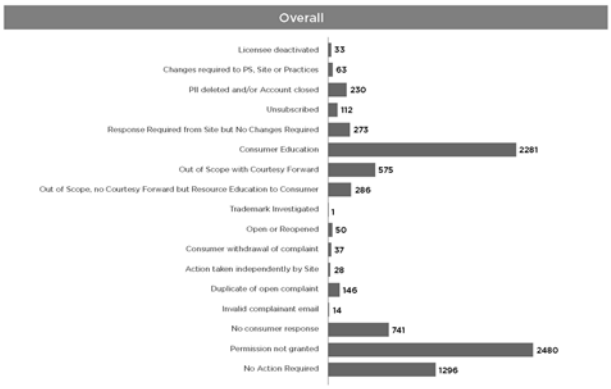
3. Consumer Complaints Organized by Outcome (2011)

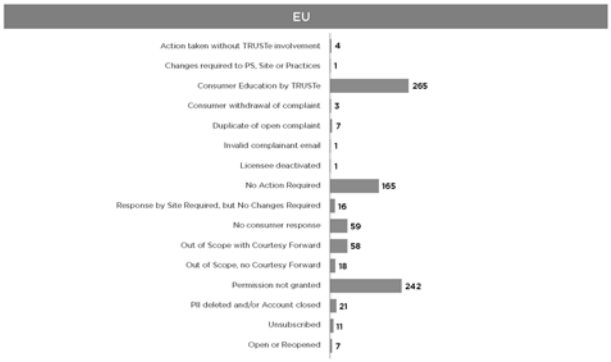
Included below are charts representing TRUSTe's 2011 consumer complaint data by outcome.

Some of the highlights of our 2011 consumer complaint data include:

- 54% of complaints were closed for procedural reasons e.g. nonsensical typing, invalid email address, consumer did not give permission for TRUSTe to pass identifying information to the site (such as needed for investigating and responding to account-specific issues).
- Of the remaining 2011 complaints:
  - 72.9% were resolved by consumer education, or courtesy forwards by TRUSTe (such as for transactional or non-privacy issues)
  - 15.7% required issue-specific research and/or data changes by the site (e.g. unsubscribe the user, close the account, remove unauthorized profile)
  - 1.6% required changes by the client to their disclosures, Privacy Statement and/or privacy practices (including duplicate complaints by different consumers about the same underlying issue)

Included below are charts illustrating the breakdown of all 2011 consumer complaints, organized by outcome:





APPENDIX – E

Consumer Dispute Resolution Process

2011 Consumer Survey Responses re: TRUSTe's Consumer Dispute Resolution Mechanism

Great!
Very good and will share with my friends
I am very happy. I received several follow-up/update emails to keep me posted on the progress of my complaint, which I found not only helpful, but also extremely considerate.
I am very satisfied.
I am so happy they could help me, and glad to remove this irritant from my life and in-basket
I was very pleased with the response, and that they made [site] finally give some sort of response to the problem.
thank you so much for helping me. it would not have gotten fixed without you
Very happy - I appreciate your help.
Absolutely thrilled if it's really resolved. I had tried every avenue to stop receiving their customer's personal info and they not only wouldn't help but were downright rude. THANK YOU THANK YOU THANK YOU
Knowledgeable, quick and courteous. I appreciate that TRUSTe was not dismissive of the issue I raised, even though I didn't explain it well the first time. TRUSTe has integrity -- they pushed the company until it got fixed.
Very efficient, did not put me aside, kept me updated on the ongoings, as professional a company who does not respond for profit.
quite satisfied
very helpful, and quick
Thank you for everything. You guys are really serieus and I will recommend you.
First of all, I would just like to thank you for the prompt service you are providing us, consumers. I just like to update my status that [site] has already helped me with my case and would no longer push this complaint to them. Then again, I want to thank the Team for the support. God bless.
Just a note to say thank you so much, [the site] contacted me after your intervention and they re-set my password for me, which means I have now regained access to my account! Once again, thanks to eCompliance for your very helpful assistance on this!
Thank you!!! You are AWESOME
Thank you very much for your professionalism in handling this matter, it is very much appreciated [...].
Thank you very much for the excellent service & prompt action you have taken regarding my compliant against [site] .. i no longer see my personal info on that website.. It is only because of your excellent service.
It seems as though whatever you have done they have "suddenly" given me access to my account- (after they told me the only thing to do was open a new account and that an operator was not going to reply to any further emails). Thank you very much for your help, your obviously that powerful that they backflipped-Many many thanks'
I would like to express my gratitude by saying Thank you for helping me out to solve this problem. I'm happy and contented with your fast response and actions. Thank you very much.
Thank you very much for resolving my complaint. I appreciate your cooperation [...]
Solid answer. Thank you for your time
thank you for yor help it has been resolved i am glad there are sites out there to help like truste

---

Mr. GOODLATTE. And, Professor Grimmelmann, you get the last word.

TESTIMONY OF JAMES GRIMMELMANN,
ASSOCIATE PROFESSOR OF LAW, NEW YORK LAW SCHOOL

Mr. GRIMMELMANN. I would like to thank Chairman Goodlatte, and Ranking Member Watt, and all the Members of the Subcommittee for inviting me to testify today. My name is James

Grimmelmann, and I am a professor at New York Law School. Although I am happy to respond to any of the Subcommittee's questions on any of its topics, my testimony today will focus on privacy.

The central goal for privacy policy online and on mobile devices must be empowered consumer choice. Good privacy technologies and good privacy laws enable people to choose whether, when and how open they want to be about their lives.

I would like to endorse three essential principles for making real consumer choice a reality. The first is usability. A choice that consumers do not know about, cannot find, or cannot understand is no choice at all. The second is reliability. A consumer who has expressed a choice is entitled to expect that it will be respected. And the third is innovation for privacy. Users benefit from good tools to help them manage their privacy.

A good example of these principles in action is social networks. Their value depends on controlled access. Everything from a private email from a mother with advice to her daughter in college to a confidential discussion group for recovering alcoholics requires sharing with some people, but not with others.

The proliferation of social networks with different technical models of sharing represents innovation for privacy in action, but that privacy must also be usable and reliable. People have lost jobs, been stalked and been splashed across the tabloids because privacy settings on social networks were too confusing for them to understand.

I am particularly concerned about what I have called privacy lurches; sudden and unexpected shifts in a social network's information-sharing practices. For example, Google mishandled the launch of its Buzz social network in 2010. Without clear warning Google exposed the names of users' email contacts to the world. This made Google Buzz, in one reporter's words, a danger zone for reporters, psychiatrists, lawyers, and everyone else for whom confidentiality is essential to their job.

The Buzz rollout violated the principle of reliability. It changed Gmail's privacy practices in a way that users could not have anticipated and that was capable of causing significant harm to them. A Federal Trade Commission investigation resulted in a settlement designed to prevent similar mistakes from happening again. And I have also suggested that privacy lurches may expose companies to legal liability for distributing an unreasonably dangerous product.

Another example of the principles is online behavioral advertising; the use of unique identifiers known as cookies to track users and to customize the ads they see. Some users appreciate receiving relevant advertising; others find the tracking creepy. Industry participants recognize this difference in opinions and offer users a choice of whether to be tracked.

One of the best ways to ensure that these choices are usable and reliable is through innovation for privacy promoting the development of tools that users can use to manage their tracking preferences and express them clearly to Web sites and advertisers. The best innovation here has come from Web browsers, antivirus software, and plug-ins that help users block and delete unwanted cookies. And the current consensus process to develop a "do not track" standard is another encouraging step.

All of these innovations can succeed only if they are respected by Web sites and advertisers. The Federal Trade Commission has taken important action against companies that circumvent users' privacy-protecting technologies, and the FTC and Congress should ensure that Web sites are not permitted to second guess users' expressed privacy preferences.

Thank you for the opportunity to speak with you today, and I look forward to your questions.

Mr. GOODLATTE. Thank you, Professor Grimmelmann.

[The prepared statement of Mr. Grimmelmann follows:]

Written Testimony of James Grimmelmann
Professor of Law, New York Law School

House Committee on the Judiciary
Subcommittee on Intellectual Property, Competition, and the Internet
New Technologies and Innovations in the Mobile and Online Space,
and the Implications for Public Policy
June 19, 2012

Mr. Chairman and Members of the Subcommittee:

Thank you for the invitation to testify today and to discuss with you these important issues of innovation, privacy, and consumer protection. My name is James Grimmelmann. I am a professor at New York Law School. My teaching and research focus on the Internet, intellectual property, and privacy law. Although I am happy to respond to the Subcommittee's questions about any of today's topics, my testimony will focus primarily on privacy.

The central goal for privacy policy online and on mobile devices must be ***empowered consumer choice***. Some people are comfortable sharing even the most personal details about their lives widely; others treasure being known well only by their close friends. Most of us fall somewhere in between, revealing some things about ourselves to some people some of the time. Good privacy technologies and good privacy laws enable people to choose whether, when, and how open they want to be about their lives. I would like to endorse three essential principles that I consider indispensable for making real consumer choice a reality.

- The first is ***usability***. A choice that consumers do not know about, cannot find, or cannot understand is no choice at all. Privacy interfaces must be clear and clearly disclosed.

- The second is is ***reliability***. A consumer who has expressed a choice is entitled to expect that it will be honored. This is true whether she has chosen to share or to keep private.

- And the third is ***innovation for privacy***. Users benefit from good tools to help them manage their privacy. Privacy policy should encourage the development of these technologies, and protect them from interference.

These principles are simple and broadly applicable. In my scholarship, I have discussed their application to a number of privacy challenges. Today, I will focus on three: personal information on social networks like Facebook, behavioral tracking of web and mobile users, and video rental records on the Internet.

Information-Sharing on Social Networks

Social networks are one of the great success stories of Internet innovation in the last decade. Many millions of Americans use these networks to share the daily joys and of their lives with family and friends, to connect with colleagues for professional projects, and to express their creative talents for appreciative worldwide audiences. In many cases, the value of these networks depends on controlled access: the ability of users to limit their communications to a particular audience. Everything from a private email with advice from a mother to her daughter in college to a collaborative spreadsheet shared among four co-workers to a confidential discussion group for recovering alcoholics requires sharing with some people but not others.

This is innovation for privacy in action. The proliferation of social networks demonstrates vividly the intense consumer desire for sharing mechanisms that fit their personal preferences. Technology companies need to be free to develop new controlled-access sharing models, and to explain their benefits to users.

Crucially, however, social networks must also satisfy usability and reliability in their privacy practices. Users who misunderstand how their information will be shared can be badly hurt if it leaks and is misused. Mishandled personal information can cause embarrassment and fear; stalkers and harassers revel in the revealing details they can discover from misconfigured social networks. People have lost jobs and been splashed across the tabloids because Facebook's privacy settings were too confusing to understand.[1]

It is important to recognize that in these cases the social networks themselves are rarely the direct privacy offenders. These are typically peer-to-peer privacy violations committed by one user against another: the reporter who takes unprotected personal photographs, the "friend" who forwards a message meant to be eyes-only. The social network provides the setting within which these privacy violations occur, but only in some cases does it bear responsibility for them.

One type of case in which social networks contribute to privacy harms involves usability problems, in the form of confusing privacy control interfaces. Facebook has had recurring trouble here, and the frequency with which it changes its interface contributes to the problem. A 2010 New York Times article documented more than 50 settings with 170 distinct privacy options in its controls.[2] Surveys consistently find that Facebook users'

---

[1] *See generally* James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137 (2009), *available at* http://works.bepress.com/james_grimmelmann/20/.

[2] Nick Bilton, *Price of Facebook Privacy? Start Clicking*, N.Y. TIMES, May 12, 2010, at B8, *available at* http://www.nytimes.com/2010/05/13/technology/personaltech/13basics.html.

privacy settings are different than what the users think they are.[3] That is, users are sharing with more people than they wish to, without understanding that they are. In an earlier version of the interface, for example, listing yourself as being located in "New York" would make your posts and photographs were visible to the millions of other Facebook users in New York.[4]

An even more troubling problem concerns what I call privacy "lurches": sudden and unexpected shifts in a social network's information-sharing practices. Lurches threaten the reliability of users' choices about privacy. A particularly egregious example was Google's 2010 rollout of its Buzz social network. Here is how I described the problem in an article:

> Buzz users post items such as photos, videos, random thoughts, and hyperlinks in order to share them with others. These items can then be viewed and commented on by other Buzz users. What differentiates Buzz from a blog is its tight integration with e-mail. Gmail users can receive Buzz updates the same way they receive regular e-mails, and reply to them too, all within Gmail. Google also built social networking features into Buzz at a deep level: choosing other users whose updates you want to follow is as easy as clicking a checkbox to let Buzz import your list of most-e-mailed contacts from Gmail.
>
> It was this last design decision that caused the privacy trouble. Google also required Buzz users to set up public profile pages that listed their Buzz contacts. Turning on Buzz, therefore, automatically published a list of users' most-emailed Gmail contacts. In Nicholas Carlson's words, this step "made Google Buzz a danger zone for reporters, mental health professionals, cheating spouses and anyone else who didn't want to tell the world who they emailed or chatted with most." For a business lawyer conducting confidential negotiations or a criminal lawyer corresponding with witnesses, this kind of exposure could easily be a sanctionable violation of client confidences. . . .
>
> As a political analyst put it, "If I were working for the Iranian or the Chinese government, I would immediately dispatch my Internet geek squads to check on Google Buzz accounts for political activists and see if

---

[3] *See, e.g.* Michelle Madejski, Maritza Johnson, & Steven M. Bellovin, *A Study of Privacy Setting Errors in an Online Social Network*, PROCEEDINGS OF THE 4TH INTERNATIONAL WORKSHOP ON SECURITY AND SOCIAL NETWORKING (2012), *available at* https://www.cs.columbia.edu/~smb/papers/fb-violations-sesoc.pdf; Alessandro Acquisti & Ralph Gross, *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*, PRIVACY ENHANCING TECHNOLOGIES: 6TH INTERNATIONAL WORKSHOP, PET 2006, at 36 (2006), *available at* http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf.

[4] *See Facebook Members Bare All on Networks, Sophos Warns of New Privacy Concerns*, SOPHOS (Oct. 2, 2007), http://www.sophos.com/en-us/press-office/press-releases/2007/10/facebook-network.aspx.

they have any connections that were previously unknown to the government."[5]

The Buzz rollout was a privacy lurch, one that violated the principle of reliability. It took software with a clearly defined privacy model—Gmail—and used personal information in a sharply different and less private way that users could not have anticipated and that was capable of causing significant harm to them. The Federal Trade Commission investigated Google over this incident and reached a settlement that includes independent audits of Google's privacy practices.[6]

I have also argued that privacy lurches of this sort may potentially expose companies to legal liability for distributing an unreasonably dangerous product.[7] Just as the maker of a defective lawnmower whose blade injures a consumer's hand will be held accountable, so too should the maker of a defective social network whose sharing settings injure a consumer's privacy. Lawnmowers and social networks are both valuable products offering consumers important benefits, but it is important that they be designed with real-world safety in mind, and law must ensure that they are.

An important special case of information sharing is when the third party is the government. Information posted to social networks is becoming increasingly useful as evidence in criminal prosecutions. Police and prosecutors have used Facebook and MySpace posts to disprove alibis, to establish gang membership, to prove violations of parole, and even to demonstrate a defendant's attempt at witness tampering.[8] These are valuable uses, and the question is how to balance law enforcement's need for access with users' legitimate expectations of privacy.

Fortunately, the Fourth Amendment establishes an appropriate baseline. The Sixth Circuit's 2010 decision in *United States v. Warshak* established that users have a reasonable expectation of privacy in the contents of their emails stored with Internet service providers.[9] Some communications via social networks, such as Facebook private messages sent to a single user, are closely akin to email. Under *Warshak*, law enforcement is entitled to obtain the contents of these messages from social network providers only with a valid search warrant. This is the right result. It respects the traditional consensus in favor of communications privacy while preserving law enforcement's ability to obtain the messages on a showing of probable cause.

Other information posted through social media is not intended to be private in the same way. I have a Twitter account that I use to comment on legal issues. My communications are intended to be seen by anyone on the Internet who is interested.

---

[5] James Grimmelmann, *Privacy as Product Safety*, 26 WIDENER L.J. 793, 823–24 (2010), *available at* http://works.bepress.com/james_grimmelmann/27/.

[6] *See In re* Google Inc., No. C-4336, 2011 WL 5089551 (F.T.C. Oct. 13, 2011).

[7] *See* Grimmelmann, *supra* note 5.

[8] *See, e.g.*, Griffin v. State, 419 Md. 343 (2011).

[9] 631 U.S. 266 (6th Cir. 2010).

These are not private information, and I understand that by posting them I have voluntarily shared them with the world. But this fact does not make anything on Twitter fair game. Some users have "protected" accounts and make their communications visible only to a controlled list of other users; other users, myself included, send private "direct messages" that are only visible to the recipient. The courts are currently engaged in the process of sorting through users' expectations of privacy in different kinds of social network information. This is a valuable evolutionary process that should continue. It would be a mistake to attempt to legislate specific technological details in this era of rapid innovation.

One trend, however, is troubling. In the recent case of *People v. Harris*, a New York state court granted a prosecutor's subpoena for all of the user information associated with a Twitter account.[10] Part of the court's reasoning was that the defendant did not even have standing to challenge the subpoena because the defendant's content was "not his" under Twitter's user agreement. This was a misreading of the limited and nonexclusive copyright license in Twitter's user agreement, which left ownership of the posted content with Twitter's users. Worse, the court's opinion would set a dangerous precedent that information sent via online intermediaries would automatically become non-private information outside of the Fourth Amendment's protection simply because the terms of service give those intermediaries the ability to use and transfer that information as part of providing their services. Packages do not become public simply because they are handed to FedEx for delivery; neither should communications handed to online intermediaries for delivery.

Twitter's response to this decision was admirable. Not only did it intervene to assert the user's privacy rights in the information the court had mistakenly decided belonged to Twitter, it amended its Privacy Policy to state, "However, nothing in this Privacy Policy is intended to limit any legal defenses or objections that you may have to a third party's, including a government's, request to disclose your information."[11] Congress should ensure that other online intermediaries are not placed in the same position by amending the Stored Communications Act so that the compelled disclosure of information not readily accessible to the general public requires a search warrant based on probable cause. This standard is technologically neutral and would provide clear and effective guidance for users, service providers, and law enforcement. It accords with common user expectations and makes the choice to depend on a social network's privacy protections both usable and reliable.

Browser Cookie Tracking of Users

Another good example of the principles in action is online behavioral advertising. Advertising companies place unique identifiers known as "cookies" on users' computers to track them from one session to another and from one website to another. The resulting

---

[10] __ N.Y.S.2d __, 2012 WL 1381238, 2012 N.Y. Slip Op. 22109 (N.Y.C. Crim. Ct. Apr. 20, 2012).
[11] *See Twitter Privacy Policy*, TWITTER (effective May 17, 2012), https://twitter.com/privacy.

profiles are used to target ads to consumers based on the websites they visit. Technology enthusiasts, for example, see ads for the latest gadget, rather than the latest tracksuit.

Some users appreciate receiving ads customized for them; others find the tracking creepy and offensive. Most reputable participants in the online advertising industry recognize this difference in opinions and offer users a choice of whether to be tracked or not. Unfortunately, these choices all too frequently fall short of the three essential principles of empowered consumer choice I have mentioned.

I am particularly concerned that some actors in the online advertising ecosystem are working to thwart the development of effective privacy-protecting technologies. A good example of one such technology is browser-based cookie blocking. All major web browsers offer users the ability to set a global policy on which kinds of cookies to accept under what circumstances. These user preference options have evolved from the confusing and blunt choices of the 1990s into thoughtful, well-balanced, and usable systems. In addition, third-party browser add-ons, such as Ghostery, provide users with easy-to-use tools for understanding cookies and automatically blocking unwanted ones.

These tools represent the best tradition of technological innovation. Companies compete to offer users more effective control over their online presence. The winners are the ones who offer the most usable products that best enable consumers to reveal what they want to reveal while keeping private what they want to keep private.

Too many advertising and technology companies treat these expressions of user preference as an inconvenient obstacle to be overcome, rather than genuine user choices deserving of respect. One form of this disdain for user preferences involved cookie variants with colorful names like "Flash cookies," "zombie cookies," "respawning cookies," and "supercookies." These terms describe a wide variety of technical practices with a common aim: ensuring that any deleted cookies are promptly replaced.

For example, imagine that Chris, a user concerned about his privacy who wished not to be tracked, followed the advice web users had been receiving for years, and deleted his cookie from the online television site Hulu.com. Unfortunately for Chris, this regular "HTTP" cookie was not the only cookie Hulu used. A program running on Hulu.com also set a "Flash" cookie on Chris's computer. When this program detected that Chris's HTTP cookie was gone, it used the Flash cookie to "respawn" the HTTP cookie. It was as though Chris had never taken action; Hulu completely thwarted his attempt to protect his privacy.

There is no good justification for this practice. Chris and other privacy-conscious users expressed their privacy preferences in their actions. A website that encounters a missing cookie should respect the user's likely desire for privacy, not surreptitiously attempt to thwart that desire. What Hulu did with respawning cookies violated all three principles of user empowerment. It made consumers' privacy choices less usable by making it harder for users to discover all the cookies they needed to remove to avoid being tracked. It made consumers' privacy choices less reliable by undermining the cookie

choices they did made. And it hurt innovation for privacy by circumventing the tools users employed to control cookies on their computers.

The use of respawning cookies became the subject both of Federal Trade Commission enforcement action[12] and of industry self-regulatory efforts.[13] Unfortunately, many companies have not accepted the basic lesson of the cookie wars: respecting users' choices. I will briefly describe three further examples in which this lesson has gone unheeded: Google's circumvention of the cookie blocker in Apple's Safari browser, numerous apps' circumvention of privacy-protecting policies on the iPhone, and recent controversy about Do Not Track defaults.

Google and Safari: Apple's Safari web browser has an important user-protective feature: by default, it blocks the "third-party" cookies that track users from one website to another. Apple advertises this feature as a benefit of Safari; some users specifically chose Safari because of it.[14] Safari still allows websites to set "first-party" cookies, which websites rely on for features like shopping carts and to keep users logged in. Google and three other advertising companies discovered a way to make third-party cookies look like first-party cookies to Safari — in essence by tricking Safari into thinking that the user had clicked on something she had not.[15] Google used the trick to combine its advertising network with its Google+ social network. It had the effect of undermining Safari's privacy promises about cookie-based tracking. Bloomberg News has reported that the Federal Trade Commission is investigating.[16]

iPhone User Information: The Apple iPhone's runaway success has been fueled by the more than 700,000 apps available to users. Many of these apps, however, are careless with user data. When users ran the social network app Path, for example, it accessed their entire address books, then transmitted everything in them to Path's servers, without using encryption to protect users from malicious hackers, and all without notice to the user.[17] This and other privacy-violating techniques were prohibited by Apple's rules for apps, but many developers came to a "quiet understanding" that they could get away with it.[18] I am

---

[12] *See In re* ScanScout, Inc., No. C-4344, 2011 WL 6800915 (F.T.C. Dec. 14, 2011).

[13] *See, e.g. FAQs*, NETWORK ADVERTISING INITIATIVE, http://www.networkadvertising.org/managing/faqs.asp (last visited June 15, 2012) (discussing NAI policy against use of Flash cookies).

[14] *See What Is Safari?*, APPLE, http://www.apple.com/safari/what-is.html (last visited June 15, 2012).

[15] *See* Julia Angwin & Jennifer Valentino-DeVries, *Google's iPhone Tracking*, WALL ST. J., Feb. 17, 2012, at A1, *available at* http://online.wsj.com/article/SB10001424052970204880404577225380456599176.html; Jonathan Mayer, *Safari Trackers*, WEB POLICY, http://webpolicy.org/2012/02/17/safari-trackers/ (Feb. 17, 2012).

[16] *See* Sara Forden, *Google Said To Face Fine by U.S. over Apple Safari Breach*, BLOOMBERG NEWS (May 5, 2012), *available at* http://www.bloomberg.com/news/2012-05-04/google-said-to-face-fine-by-u-s-over-apple-safari-breach.html.

[17] *See* David Sarno, *Phone Apps Dial Up Privacy Worries*, L.A. TIMES, Feb. 16, 2012, at A1, *available at* http://articles.latimes.com/2012/feb/16/business/la-fi-app-privacy-20120216.

[18] Dustin Curtis, *Stealing Your Address Book*, DCURTIS, http://dcurt.is/stealing-your-address-book (Feb. 8, 2012).

concerned about a Silicon Valley culture in which behavior that is illegal, unethical, and expressly forbidden is nonetheless considered routine, and I support greater enforcement efforts against mobile app companies that consciously ignore the privacy rules of mobile app platforms.

Do Not Track Defaults: An open and participatory multi-stakeholder process is underway to define a "Do Not Track header": a flag that a user's web browser could set to indicate a request that the user's online activities not be tracked by the website that receives the request.[19] This is an important and valuable initiative, but it will only succeed if the Do Not Track request is usable and respected. Microsoft recently took a valuable step towards that goal by announcing that Do Not Track would be on by default in the next version of its Internet Explorer browser.[20] I consider this move an excellent example of innovation for privacy. Users benefit from being able to delegate the choice to enable Do Not Track to Internet Explorer; it simplifies the option of choosing this form of privacy. Microsoft will succeed in the competitive browser market if and only if users consider this a valuable feature. But some other participants in the Do Not Track process, including representatives from Yahoo! and Google, have been pressing for the ability to disregard the Do Not Track request if it comes from a browser, like Internet Explorer, in which it is on by default.[21] This attempt to sabotage the practical usability of Do Not Track would make it pointlessly harder for consumers to express their privacy preferences. Congress should legislate full compliance with Do Not Track — which means that websites may not second-guess properly expressed user requests.

Video Record Privacy

A final example of this framework in action is the Video Privacy Protection Act ("VPPA"), enacted in 1998 to ensure privacy in consumers' video rentals. It prohibits the disclosure of the videos rented or purchased by an individual without that person's consent.[22] In many respects, the VPPA is a model privacy statute. It gives consumers confidence that personally sensitive information will remain confidential. Its commands are backed up by forceful but reasonable penalties. Its requirements are specific and clear, so that companies know when it applies to them and when it does not, and know what they need to do to comply. For all of these reasons, the VPPA does an excellent job of ensuring reliability.

As an example, in 2007, when Facebook introduced its Beacon feature, users' actions on other websites, such as the recipes they clipped on Epicurious, were

---

[19] *See generally Tracking Protection Working Group Charter*, WORLD WIDE WEB CONSORTIUM, http://www.w3.org/2011/tracking-protection/charter.html (last visited June 15, 2012).
[20] *See* Brendon Lynch, *Advancing Consumer Trust and Privacy: Internet Explorer in Windows 8*, MICROSOFT ON THE ISSUES, http://blogs.technet.com/b/microsoft_on_the_issues/archive/2012/05/31/advancing-consumer-trust-and-privacy-internet-explorer-in-windows-8.aspx (May 31, 2012).
[21] These views are detailed in the archives of the Tracking Protection Working Group's public mailing list at http://lists.w3.org/Archives/Public/public-tracking/.
[22] 18 U.S.C. § 2710.

automatically posted to Facebook.[23] This broke users' implicit privacy model of the Internet; it thwarted their expectation that what happens on Epicurious stays on Epicurious. The minimal notices Facebook provided were easy to miss, and it opted users into Beacon without their consent. I very much doubt that most of us would like the food we cook, the books we read, and the movies we watch to be automatically trumpeted to all our friends and acquaintances.

Most of the companies that partnered with Facebook in this privacy mistake escaped being held accountable for their actions due to the lack of clear general online privacy laws. The one exception was Blockbuster, and it faced up to its responsibility because the VPPA gives such unambiguous direction. A class-action lawsuit against Facebook and Blockbuster resulted in a $9.5 million settlement.[24]

Significantly, the VPPA provides consumers with genuine choice. While it sets a default of privacy, it specifically excepts any disclosure made "with the informed, written consent of the consumer given at the time the disclosure is sought."[25] If a video site would like to share with a user's friends the fact that she just watched and loved *Wall-E*, all it needs to do is ask. If a user would like to share this fact with her friends, all she needs to do is tell the site that it is okay to share. The VPPA understands that some users will choose to share, and others will choose not to.

In the last year, some critics have questioned the usability of this choice. The VPPA's requirement that consent must be given "at the time the disclosure is sought" means that users cannot give blanket, up-front permission for their video views to be shared. It does not matter how clearly Netflix explains this sharing to users, or how unambiguously they say that the sharing is okay, the VPPA still prohibits advance consent. I can share with my friends on Facebook the titles of all the songs I listen to on Spotify, but I cannot share the titles of all the movies I watch on Netflix. This is a usability issue: the VPPA does not offer a usable general choice in favor of sharing. H.R. 2471, which passed the House in December, would amend the VPPA to permit advance consent.

While I am sympathetic to H.R. 2471's goal of enabling genuinely symmetric consumer choice, I am concerned about how it achieves that goal. Consent given at the time of disclosure requires relatively straightforward notice. The provider can explain the specific disclosure it is about the make, and the consumer can understand the full scope of the disclosure. But consent given in advance requires more detailed notice in order for the consumer to give genuinely "informed" consent. If you ask for my consent to say on Facebook that I have just watched *Schindler's List*, I will understand that you are about to post a single, specific item to tell my friends on Facebook that I watched . . . *Schindler's List*. If you ask for my general consent up front, then I will need both to anticipate what kinds

---

[23] *See* Louise Story & Brad Stone, *Facebook Retreats on Online Tracking*, N.Y. TIMES, Nov. 30, 2007, at C1.
[24] *See* Lane v. Facebook, No. 5:08-CV-03845-RS (N.D. Cal. settlement approved Mar. 17, 2010).
[25] 18 U.S.C. § 2710(b)(2)(B).

of movies I might watch, and also what kinds of services you may share it with and how you will share it.

These uncertainties over what counts as "informed" advance consent will undermine the VPPA's admirable clarity. Consumers deserve specific guidance about the kinds of sharing that will take place if they click "yes." If the VPPA is to be amended to permit advance consent, it should require video providers to give that specific guidance, and state that advance consent is permissible only for identified classes of disclosures to specifically named partners.[26]

[26] For more on the VPPA and H.R. 2471, *see generally The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century: Hearing Before the Subcomm. on Privacy, Tech., and Law of the Senate Comm. on the Judiciary*, 112th Cong. (2012) (testimony of William McGeveran), *available at* http://www.judiciary.senate.gov/pdf/12-1-31McGeveranTestimony.pdf.

Mr. GOODLATTE. I will now begin the questioning of the witnesses.

I believe that consumers have the relevant information about—if they have the relevant information about privacy policies, they will make informed decisions about how to allow their information to be used, and will choose what services to use in part based on

their comfort level with those privacy policies. I would like to ask each of you what your organization is doing specifically to make privacy policies more transparent and easier for consumers to understand. And we will start with you, Mr. Shipman.

Mr. SHIPMAN. Sure. Thank you.

The expectations in managing privacy with consumers is a never-ending battle. It is not something that you can simply come out with a particular policy and say, "Okay, we have written this as clearly as possible, and we can rest on our laurels." So this is something that continues to evolve.

From the inception of eBay's privacy program, we have actually created in 1998 a chart, and at the time it was fairly simple, because you could have a chart with three or four classifications or groups of entities that you share information with.

Mr. GOODLATTE. I am going to have to get you to get to the point because I have got several questions and several witnesses to answer. So tell us what you are doing right now and prospectively.

Mr. SHIPMAN. Absolutely. The focus right now is around bringing icons, bringing specific logos or vignettes, whether it is via video or other types of embracing new technology, to be able to answer questions the customers have. AdChoice is a perfect example where we have links there embedded into advertising and through other types of things like that.

Mr. GOODLATTE. Excellent.

Mr. Reed?

Mr. REED. So we have an interesting situation in that we represent the developers. And so we have been trying to give developers tools. We have run a series of privacy boot camps where we spend the entire day focusing on getting a developer from walking in the door, saying, "Okay, I need this privacy policy," to when they walk out the door not only having privacy, but understanding the tools they need to have to have a narrative with their customers.

And very specifically, one of the ones I would like to highlight is our work with Moms With Apps, where we have created a set of icons that have been adopted by some of the privacy policy generators, including Privacy Choice, and in talks with TRUSTe as well, so the developer can select the icons immediately when they build their privacy policy so when it shows up for the user, bam, they can see it. It doesn't collect information, it doesn't link to the Web, or it does.

So, one, we have to empower developers; and, two, we are working on building tools to inform our customers what those privacy policies mean.

Mr. GOODLATTE. Thank you.

Mr. Babel.

Mr. BABEL. Sure.

So TRUSTe helps Web sites through a privacy policy generator generate their first privacy policy. Big companies might have attorneys that do that; small companies, start-ups, three people in their garage need help. Particularly around mobile applications we find that is critical. As I mentioned in the testimony, about a third of mobile applications even have a privacy policy today, so we are really trying to help people start by having a privacy policy.

The second thing we do is once people have privacy policies, we help make certain that they are good, of high quality, clear, transparent, easy to read, easy to understand, and that is where we help the company have a certified privacy policy where we say it meets a good high bar, and that the company is following and actually doing what their privacy policy states.

Mr. GOODLATTE. Thank you.

Mr. Reed, many Internet services are free and are monetized through targeted ads and data collection. How much would app prices go up, or what would it cost to use a search engine or social media Web site if companies were restricted from the data that they could collect?

Mr. REED. Well, I think we have to look at two sets of numbers: One, what is the change in the way that we develop apps; and, two, when it comes to the actual impact on the industry. If you remove all ads altogether, I think you would see some enormous impacts. If you remove strictly ads that use information, and you just do context-based ads, the estimates run about 20 percent, a loss of about 20 percent of income for those that are ad supported.

The reality is that the model right now, we are looking at trying to make sure that we get apps that we get paid directly and supplement through advertising. So it probably would cost us about 20 percent of revenue.

Mr. GOODLATTE. Mr. Babel.

Mr. BABEL. I think one of the key unique factors in mobile versus Web sites, just to point out quickly, is that mobile actually has a monetization mechanism where you can go back to the extent that someone were to opt out of ad targeting and go back and say, I am limiting the features of this mobile app and pushing you to a charged version. In the Web site version of the world in that ecosystem, 15 years ago we started giving out free content online, and it would be very hard to go back to that paywall.

As we have read industry research, although I haven't done it ourselves, we have seen similar numbers to those that Morgan has proposed in terms of the drop-off in advertising, but it is not something that we have tracked and have estimated directly.

Mr. GOODLATTE. Let me ask the three of you what your greatest concerns are about the European Union's recent efforts to impose a regulatory regime in Europe.

Mr. Shipman.

Mr. SHIPMAN. I think the challenge within the EU is certainly that we are looking for standards that create international operability, and so any change in one particular region for a global company destabilizes that operability. And while we certainly have received approval through the binding corporate rules for operations in Europe and used that as our global standard, changes in that and more restrictions in that certainly make that much more difficult for us.

Mr. REED. We are short on time, so I am going to echo Chairman Smith when he said the problem we have with it is just the same. We are not two developers in a garage—we are two developers in a garage, not two developers and a lawyer. The difference between us and Europe will create a lot of difficulties for our developers.

Mr. GOODLATTE. Mr. Babel.

Mr. BABEL. Yes. Our clients, whether they be domestic clients or international clients, are challenged by the fact that there are just different requirements by country. And when you are a big company and trying to manage your portfolio of Web sites across users from each different region, it is challenging to implement technologies to address that. It is a lot of hard work; it is a lot of hard work up front.

And to be honest with you, most companies have not met the deadline for the U.K. Cookie Audit Compliance that was May 25. In fact, most government agencies in the U.K. have not met that deadline as well. So it gives you a sense for the challenges that are involved with this policy implementation.

Mr. GOODLATTE. Mr. Grimmelmann.

Mr. GRIMMELMANN. As the others have mentioned, the lack of harmony across many countries is a significant problem, and it leads to situations in which especially the small players have difficulty even finding out all the laws they need to comply with.

Mr. GOODLATTE. Thank you.

The gentleman from North Carolina Mr. Watt is recognized.

Mr. WATT. Thank you, Mr. Chairman.

The Ranking Member of the full Committee Mr. Conyers raised a difficult issue that I want to ask some questions in here relating to legislation versus self-regulation. The Administration's blueprint contemplates baseline legislation complemented by a self-regulatory model to implement the Consumer's Bill of Rights. So let me ask a couple of questions in this area.

Do we, in fact, need a Federal Consumer Bill of Rights or something maybe not called that, but some Federal baseline in this area to deal with privacy? And if not, two questions arise. Wouldn't that leave it open in this Internet thing, which clearly is across State borders, for State by State by State to enact legislation? And wouldn't that leave it open for self-regulation, which is okay if people behave, but is not all that enforceable if people do not behave, I guess is the question?

So Mr. Shipman, Mr. Reed, Mr. Babel, and Professor, if you can address those couple of questions in there, I would be appreciative to you.

Mr. SHIPMAN. Absolutely. And thank you for the question.

I think the challenge, as you highlight, is, with self-regulation, it leaves customers with uncertainty. eBay has long supported a Federal omnibus privacy bill, and the key reasons for that are largely to provide the small and large businesses that we do business with to provide that level of certainty.

Mr. WATT. So you think there should be a Federal standard of some kind.

Mr. SHIPMAN. Yes, we do.

Mr. WATT. Yeah. Okay.

Go ahead.

Mr. REED. Yes, we have been active supporters of the NTIA effort. And I do think, as we get through this, we should talk about ways that the government can enforce bad behavior. I definitely think that is something where, from in particular a small business, it is very important to see the government step in and bring harsh

actions against companies that do violate people's privacy, because nothing gets the message clearer to our members.

Mr. WATT. Of course, the first step is to have a clear set of rules about what the standards are.

Mr. REED. Yes, exactly.

Mr. WATT. Okay.

Mr. REED. And so, yes on that, good on enforcement.

Mr. WATT. Okay.

Mr. BABEL. I think we have seen at TRUSTe self-regulation work, and work effectively. And, in particular, over the last few years, with the beginnings of the DAA effort around AdChoices, you have seen self-regulation accelerate quite rapidly in the last few years to reach out and touch consumers and give them——

Mr. WATT. So what happens in self-regulation if you have self-regulation and you or your members or your customers or clients don't live up to what they agreed? What remedies do I have to enforce that, or who enforces those standards?

Mr. BABEL. Sure. So, in TRUSTe's case, where we certify companies for good privacy, the first thing we do if there is an issue with one of those clients is help them get back into alignment with our guidelines for——

Mr. WATT. Got that, but——

Mr. BABEL. If——

Mr. WATT [continuing]. My data is already out there at that point. So how do I get a remedy?

Mr. BABEL. The second thing we do is eliminate them from the program. And, in fact, last year we eliminated——

Mr. WATT. That still doesn't give me a remedy.

Mr. BABEL. The third remedy that we have put in place to the extent that there is egregious behavior, is we have, in fact, referred people to the FTC. And the FTC has taken action in some——

Mr. WATT. So there has to be a Federal standard.

Mr. BABEL. There has—yes, we have——

Mr. WATT. Okay. All right. Okay. I am——

Mr. BABEL [continuing]. Refer to it——

Mr. WATT. We are back there. All right.

Go ahead, Professor.

Mr. GRIMMELMANN. A Federal baseline would first bring important clarity to the area. And, in addition, all of the processes of consumer choice and bargaining, where Web sites offer bargains to users and explain the tradeoffs, only work if the consumers have an entitlement to their privacy to begin with. If we don't have a baseline, then they don't need to respect it.

Mr. WATT. All right.

Now, is there anybody out there in the industry that is advocating for no Federal baseline? Are there any voices out there, or do you all represent pretty much the standard belief? If so, it seems to me we can quit vexing about whether we need a baseline and start vexing about what we put in the baseline. Is that right? Anybody out there got a different opinion about this, I mean, I guess is the question.

Mr. REED. I guess the only nuance that I would add is that the good partabout what NTI is doing—and it will be a lot of work—is that it is being built bottom-up as a multi-stakeholder effort,

where we are going through long, intense meetings talking about the meanings of words and the definitions. So it is actually working from the standpoint of what technology is capable of doing and gives us the option to change it as we become capable of doing new things.

So I think it is important that it not be a government-imposed, top-down pressure, but it be developed by technologists as a way to handle when we change our stuff.

Mr. WATT. In the meantime, are the laws that are already out there—I mean, I assume there are gaps. Are there laws that are already out there that provide some kind of protection?

Mr. REED. I would say it's more than some.

Mr. WATT. Yeah.

Mr. REED. I think the Federal Trade Commission has already shown that it has some teeth. We obviously have regulation on HIPAA. We have regulation Gramm-Leach-Bliley. So, depending on what kind of data you have, there are more than a fair number of regulations.

Beyond that, this Committee knows we also have antitrust laws to deal with companies that are large players that cavalierly disregard people's privacy time and time again. So if you can't curb behavior through FTC, you can always go and look at antitrust as well.

Mr. WATT. Mr. Chairman, my time has expired, but, as I told the Chairman, I am going to have to leave to go over and hear Jamie Dimon testify in my other Committee. So let me make a unanimous consent request before I leave, Mr. Chairman, to offer into the record the February 2012 White House green paper, "Commercial Data Privacy and Innovation in the Internet Economy: Dynamic Policy Framework;" number two, a March 2012 FTC proposal, whatever, report, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers;" and a March 2012 report, "Search Engine Use 2012," a project of the Pew Research Center.*

Mr. GOODLATTE. Without objection, those will be entered into the record.

And I will turn the Chair over to the Chairman of the Committee.

Mr. SMITH [presiding]. Mr. Babel, let me address my first question to you. Actually, you have already answered my initial question in response to a question by Mr. Watt, but I wanted to follow up on the idea of how enforcement worked when it came to individual online businesses that might violate the best practices. And you responded to Mr. Watt and said, ultimately, if there was a clear violation and there wasn't any response, you would refer online businesses to the Federal Trade Commission, I think. Have you ever had occasion to do that?

Mr. BABEL. Yes, we have.

Mr. SMITH. In how many instances?

---

*The submissions referred to are not reprinted in this record but are on file with the Subcommittee and can be accessed at:

http://www.whitehouse.gov/sites/default/files/privacy-final.pdf;

http://www.ftc.gov/os/2012/03/120326privacyreport.pdf; and

http://pewinternet.org/~/media//Files/Reports/2012/PIP__Search__Engine__Use__2012.pdf

Mr. BABEL. There has been one instance that is in my knowledge, one instance in 2008 of a company called Classic Closeouts, which——

Mr. SMITH. And what did the FTC do?

Mr. BABEL. They took action. It was settled I think late last year with a $2-million-plus finding.

Mr. SMITH. Okay. And how many online businesses, in your judgment, have violated the best practices that you have endorsed?

Mr. BABEL. So, last year in our written testimony we provided something we call the transparency report, where we walk through number of customers and number of certifications.

Mr. SMITH. Right.

Mr. BABEL. And each year I think there is two important data points. One is the number of companies that come to us for certification and never get certified because they don't pass the standard to begin with. And that is about 8 to 10 percent of all the clients that are approaching us for certification never meet the bar. The second thing is that, in last year, 11 companies violated, kind of, what we think are best practices——

Mr. SMITH. Okay. And of those 11, you referred 1 to the FTC?

Mr. BABEL. Not last year. The referral to the FTC was in a prior year.

Mr. SMITH. Right. Okay. Thank you, Mr. Babel.

Mr. Shipman, let me address a question to you and perhaps to Professor Grimmelmann as well. And it is this: We have heard, I think, from all witnesses today about the need for online businesses to protect consumer data. My question goes a little bit farther. Should consumers be able to find out what personal data has been gathered about them?

Mr. SHIPMAN. Absolutely. And, in fact, within our corporate standards that we have had approved through Luxembourg, that is a requirement that we meet.

Mr. SMITH. Okay.

Do any of the witnesses today feel that consumers should not or do not have a right to know what personal information has been gathered about them?

Okay.

Next question is, should consumers be able to opt out of the process that gathers that personal information about them?

Mr. Shipman, what do you think?

Mr. SHIPMAN. I am going to give you a multipart answer on that one.

Mr. SMITH. Okay.

Mr. SHIPMAN. There are certain components of collection that are required. eBay certainly has financially related institutions.

Mr. SMITH. Uh-huh.

Mr. SHIPMAN. We process financial transactions as well as all kinds of e-commerce transactions and commerce.

Data that is essential for the safety, security, antifraud, in that area, we cannot allow consumers to opt out of. Certainly, for marketing purposes and other types of secondary uses, we can allow——

Mr. SMITH. You would allow them to opt out. Okay. Thank you.

Professor Grimmelmann, do you have an opinion on that?

Mr. GRIMMELMANN. In the context of first-party collection, where the consumer is dealing with a Web site——

Mr. SMITH. Yes.

Mr. GRIMMELMANN.—Mr. Shipman expresses a very clear and correct view.

Mr. SMITH. And you agree with him. Okay.

That concludes my questions. The gentleman from Michigan, the Ranking Member of the full Committee, is recognized for his questions.

Mr. CONYERS. Thank you, Chairman.

Mr. Reed, we have heard a lot about self-regulation here—too much, as far as I am concerned. I don't know what you think this Committee—what others, not you, think, that we make rules, we make laws, we have court decisions, and now we come up with a "let's go for self-regulation." We have been hauling—all of the big tech companies have been in and out of court repeatedly.

And so, can you give me a little more confidence about this whole notion of self-regulating?

Mr. REED. Well, I think the first thing we have to look at is, does the FTC have enough resources? We start with that. But I think you also have to look at continued behavior. There is carrot and stick, right? Industry self-reg is a carrot; do this, and you won't get the stick.

I think that for small companies, we are usually dependent on platforms, and we are incredibly responsive to our customers. Why? Because we are scared of losing them. I think one of the things that concerns us very much that has been happening in the privacy space is that some of the violations have been actually done by big companies and one in particular. You know, the Chairman brought up Wi-Spy. That trickles down into the sentiment of the regular citizenry.

So, yes, I think it is critical that the resources are at the FTC and that the DOJ is willing to step up and go after those who don't respond to carrot and don't respond to stick.

Mr. CONYERS. Yeah. But, Mr. Reed, a lot of this privacy—we don't even know what is being collected, and we don't have any way of getting at it. I mean, I see a huge problem still out here, don't you?

Mr. REED. Well, I think the question of what is being collected, I think we can actually figure out what is being collected. The larger question is, what happens to it after it is collected? What is it combined with? Does that create problems, and are people selling it in a way that is damaging or causes harm to people's privacy? Does it make it hard for them to get a job? Does it make it hard for them to buy a house?

That is really the question. It is not what is collected; it is what is done with the collection of that information after, how it is assembled. And those are areas where I think that there can be questions and we should find good answers.

Mr. CONYERS. Thank you very much.

Well, we know what is being collected. Everything. Is there anything that they—I mean, that is the nature of the problem. I——

Mr. REED. But I think it is worth noting that the Sears catalog had information on people in the 1900's. They knew what we were

buying. And it is really about what is done to harm people afterwards. That is really the kicker. Because, you know, we all had the Sears catalog as a kid in our house, and you would read it. Sears knew what you bought. They kept a record of what you bought. That was a good thing. Do you know if what they did with that information prevented you from buying a house or prevented you from getting a job or prevented you from getting insurance?

Mr. CONYERS. Or hurting your credit.

Mr. REED. Exactly.

Mr. CONYERS. Let me turn to Professor Grimmelmann for a continuation of this discussion. I mean, this is a very nice conversation we are having here with four experts, but, I mean, there is a certain element here of "let's trust everybody to do the right thing." The FTC is underfunded. Leibowitz, Jon Leibowitz, the Chair, comes before us every year and makes the case that they need more resources.

How do you see this discussion of giving benefit of the doubt to these huge companies that are collecting what we don't even—well, from my point of view, it is everything. We go back to Sears in 1900. Well, guess what they are doing now, if you think that was something.

Mr. GRIMMELMANN. I would like to say that some huge companies can play an important role in building tools that stop other huge companies from gathering lots of data. So, for example, Apple puts significant restrictions in the iPhone that limit the data that apps can collect so that the apps can't gather location data without the user's express permission. And Microsoft, in its most recent version of the Internet Explorer, will be turning on the "do not track" header by default to tell Web sites they should not collect data about users.

We can find ways to exploit the competitive process in the industry, to have companies recognize privacy is an advantage and help consumers keep personal data from other companies.

Mr. CONYERS. But there are some that are disregarding the tracking instructions of their consumers. You know that.

Mr. GRIMMELMANN. So, the advantage of that is that the company that disregards the tracking request has now done something that is explicitly deceiving the consumer and failing to respond to the request, rather than just taking advantage of their ignorance, which gives the FTC a surer basis for action.

Mr. CONYERS. Thank you, Mr. Chairman.

Mr. SMITH. Thank you, Mr. Conyers.

The gentleman from Pennsylvania, Mr. Marino, is recognized for his questions.

Mr. MARINO. Thank you, Mr. Chairman.

I am going to start with Mr. Shipman. And let's back the bus up here a little bit, if you would, please. And if anyone has anything to add to it, just chime in.

Let's start back with the scenario, a parent is having a personal conversation with their son or daughter who is off to college; or one corporation is having a confidential exchange of information with another corporation concerning, let's say, a merger. Once I hit that send button, let's educate the people of where does that go and how many people or how many entities have access to that even when

I hit the delete and the other side hits the delete? Do you understand my question?

Mr. SHIPMAN. Yeah, sure. Basically, your question, just to quickly summarize, is, when you hit send on an email, how many different entities could it possibly end up with.

Mr. MARINO. Even after I delete it.

Mr. SHIPMAN. Sure, sure.

To me, the biggest challenge here—I mean, there are many challenges. eBay is not an ISP; we actually don't provide email, but I am knowledgeable enough to be able to provide a few comments.

One of the toughest components here is access where you have other governmental agencies or law enforcement or other requests where the consumer may have no knowledge of that information being requested. Beyond the technology components, it had been deleted within the systems, within service providers, within a custodial relationship——

Mr. MARINO. Okay, I understand the law enforcement aspect of it. I have been a part of it for 19 years. So just give me your best estimate on how many entities would have that information.

Mr. SHIPMAN. Go ahead.

Mr. REED. I think, let's break it into two camps. Is your service a cloud-based, or are you just going from my company to your company? If you are going company to company, not too many entities in between will hold on to it.

But he raises the key point, which is a part of ECPA reform in these questions, is that law enforcement has stepped in to place collection points in the process——

Mr. MARINO. Okay, let's exclude law enforcement for a moment.

Mr. REED. If you exclude law enforcement, company to company, not much. If it is company to cloud provider and back, then the cloud provider does have access to that information at a certain level. Most——

Mr. MARINO. Okay. Now, if several entities, even if it is company to company, how long does that individual or that entity have that information? Until they just delete it?

Mr. SHIPMAN. So, once an email or other piece of data is received, it is within that—if it is a responsible company, they have a data classification and data retention policy. So, depending on the classification of that data, it may be 7 days, it may be 7 years.

Mr. MARINO. All right, I am going to jump to the next one then. Who best can answer this: What would prevent an employee from obtaining that information and sharing it?

Mr. REED. It depends on their status in the corporation. Somebody who has the keys to the kingdom, so to speak, the network nerd in the closet, he is going to have all of it.

Mr. MARINO. So my point is——

Mr. REED. Right.

Mr. MARINO [continuing]. People have access to it and can use it nefariously, correct?

Mr. REED. Yes. And that is—yes.

Mr. SHIPMAN. There is an important consideration here, which is, there are tools that certain companies, certainly eBay being one of them, deploys which do monitor and track access to information within the organization. So not only are employees based on per-

mission have access or don't have access to information, but also if there is anomalous activity, it is detected, reported, and prevented.

Mr. MARINO. Mr. Babel and then Professor, maybe you can give me a quick answer on this. I am an individual that questions "do we want the Federal Government involved?" In fact, I take the position that the Federal Government spends too much time in our lives to begin with.

So give me, Mr. Babel, if you can, please, give me your opinion based on the fact that—can the industry police itself? I have a little problem with the fox setting rules and regulations for the henhouse. But give me a scenario, if you would, contrast them, policing itself and needing Federal regulations.

So if you both could answer that, please. Mr. Babel?

Mr. BABEL. Sure. So I think that it is—you know, TRUSTe has self-regulatory programs. The key asset that we have is our band of consumers. So if we aren't living up to the standard of making certain that people who no longer follow the standards are out, like, for us, it is the whole company we are betting. Our credibility is the key, meaning the program and its credibility.

I think when it comes to legislation, one of the things that I am concerned about is just, you know, what are the unintended consequences of legislation? If you look at something like CAN-SPAM, even that was a law that was well-written, well-adopted, but at the end of the day, 90 percent of email is still spam. It is not the law that eliminated the spam in your inbox, it is technology.

Mr. MARINO. I am running out of time here.

Professor?

Mr. GRIMMELMANN. I think that the companies you are most going to want Federal intervention for are the ones who are not TRUSTe members who are engaged in shady, gray-area marketing, that conceal their tracks, click fraud, all kinds of shady deals that are trying to rip consumers off.

Mr. MARINO. Okay. Thank you.

I yield back. Thank you.

Mr. GOODLATTE [presiding]. I thank the gentleman.

The gentleman from Florida, Mr. Deutch, is recognized for 5 minutes.

Mr. DEUTCH. Thank you, Mr. Chairman.

Mr. Babel, you said that 59 percent of people believe that their information is protected. You touted that number. Four in 10 people are concerned that their information is not protected, I presume is the balance of that analysis, the balance of that polling.

I just want to talk about the self-regulation piece of this, which a number of you had talked about. You have a program, a privacy program, which, if I understand what you are saying correctly, if a company adopts it, then they receive your certification. Is that right?

Mr. BABEL. Correct.

Mr. DEUTCH. And has that certification been given to the largest companies? And what Mr. Shipman described sounds like a really terrific privacy policy, which I will ask about in a minute. But do they have your certification on their privacy policy?

Mr. BABEL. They are our client, yes.

Mr. DEUTCH. And do all of the—I mean, do the biggest, just thinking about those companies with market dominance, does Google have a certification, does Facebook have a certification from you for their privacy policies?

Mr. BABEL. One of the things we look at is the top 100 Web sites listed by a company called Alexa that is based on consumer traffic. And we have about 50 percent of those top 100 clients. So we have good penetration but certainly not all——

Mr. DEUTCH. All right. So just again, thinking about the ones that we use most often, does Google have a certification and does Facebook have—for their privacy policy.

Mr. BABEL. Google is not a certified client of TRUSTe, and neither is Facebook. We do work with them in some different areas, but they are not certified clients of our program.

Mr. DEUTCH. And, Mr. Reed, when you talked about the information to be collected, you said we should know what data is being collected, who we are sharing it with, and being transparent with customers.

Mr. Babel, is that a part of your certification? Do you look at each of those?

Mr. BABEL. Yeah, if we were to think of the highest three levels of the certification, the business needs to first be transparent, meaning tell people what they are collecting, you know, if they are sharing it, how long they are holding onto it. They need to give choice; would you like to not have that data being collected? And they need to be accountable to that choice.

So, yes, the tenets of what Morgan outlined are what——

Mr. DEUTCH. And I am sorry, I don't—unfortunately, I don't know—I am learning a lot today, but I don't know well enough the relationship between TRUSTe and some of the other companies. What is it? I mean, when you say you have worked with some of these other companies but they don't have the certification, do you suggest to them what is missing? Or when it comes to those three items that we just discussed, when you look at a company with real market dominance, like Google, for example, or like Facebook, is there one of those three that they might be missing? Are there certain things that we ought to be considering?

Mr. BABEL. Think of it as, it is a totally different effort that we are working on with them. I will give you the example with Google. They have a business-to-business app marketplace, where a business owner using Gmail can download an application. We certify those applications, but it is in a partnership with Google. So it is not related to, kind of, the three core tenets. We don't work with them in our core certification business. It is kind of a separate, adjacent thing.

Mr. DEUTCH. So I guess what I am really getting at is, when you talk about self-regulation and the success of self-regulation, for a company, any company that has real market dominance, is that sufficient to rely on? Do the 40 percent of consumers who are concerned their information is not kept private, should they be satisfied with the privacy policies established in a self-regulatory environment, if not every company regulates themselves the same way?

Mr. Reed, you look like you want to jump in.

Mr. REED. Well, I think you have to look at behavior. You know, eBay is sitting here. They have a pretty good track record so far on privacy. A lot of our developers use their PayPal system to enable app purchases. It has worked out pretty well. We haven't had those.

So I think your question about the size of the company is not the first test. The first test is, what are they doing? And if a company with dominance has the power to take it and kind of thumb their noses at consumers, well, then, yes, I think that is the kind of time where you have to start taking a look and you have to start asking harder questions.

So it is not the size as much as it is the behavior that really triggers this.

Mr. DEUTCH. Well, Mr. Reed, I mean, you are more familiar with the industry than I am. Are there any companies that you think are thumbing their nose at these privacy issues?

Mr. REED. Well, I mean, I think we have heard the name several times; everybody has been talking about it. I think Google has—Google's privacy violations to date have certainly raised a lot of concern. I think it is the ironic; you know, it got so bad that the Jon Stewart show, "The Daily Show," actually made fun of it on WiFi. So that——

Mr. DEUTCH. Mr. Reed——

Mr. REED [continuing]. Harms all of us.

Mr. DEUTCH. Mr. Reed, I am almost out of time. Of the three things that you point out—know the data being collected, who it is being shared with, and being transparent with those customers—which of those three do you think is most often being ignored by any company that might be thumbing their nose at these privacy issues?

Mr. REED. I think in the case of Google, I think the problem is that they haven't been transparent with what they were doing. I think that was very clear onWi-Spy. It was clear on the Buzz settlement. They haven't been transparent. And I think that is an area that they need to improve or regulators need to step in.

Mr. DEUTCH. All right. Thank you.

Thank you, Mr. Chairman. I yield back.

Mr. GOODLATTE. I thank the gentleman.

The gentleman from Utah, Mr. Chaffetz, is recognized for 5 minutes.

Mr. CHAFFETZ. Thank you. Thanks, Mr. Chairman.

And thank you for all for being here. I appreciate it.

I wanted to highlight the idea that the Internet, the tech sector is actually something in our economy that is working. You are looking at growth in jobs and expansion of our economy, this is one sector that is thriving.

One of my concerns is, while we have these deep-seated needs to make sure that privacy is protected, that we are protecting consumers, I think, Mr. Chairman, we also need to be ultra-careful in making sure that we don't convolute the process to a point where young entrepreneurs, new startups, aren't able to start because there is such a mass of regulation and uncertainty.

I do question the notion that the FTC is the right organization. I wonder—we talk a lot about the teeth of the FTC, but we can

probably count on one hand where they have actually taken action. And so I think that begs the question of, should this be done in part by statute so that we can use Article III Courts, as opposed to the FTC, which would be much more readily available to a consumer or an individual. It is just something, Mr. Chairman, that I think we need to continue to explore, because I am not convinced the FTC is the end-all, be-all.

I am also concerned that if we have multiple jurisdictions here—the Consumer Financial Protection Board, for instance—you are going to end up much like in the financial sector where you have conflicting rules and regulations.

I think it is also important that the Congress stand up for itself and not allow an Administration—I don't care which party it is involved with—allow just simple rulemaking to push through the process and not allow the back and forth and the discussion that would happen in Congress. I think we have been failing on that front in general.

There are a couple other areas that I would like you to address. And our time is so short here, but, Mr. Chairman, I think one of the things we have to further explore if we are going to truly look at privacy is how do we deal with minors. You know, my 11-year-old arguably knows more about using the apps and the Internet than most people three, four, five times her age.

We are going to also have to deal with the national versus the international aspect and scope, which is obviously for the need and the genesis of SOPA. That issue has not gone away. We are still losing billions of dollars overseas, and we are going to have to deal with that.

The other area that I am really trying to focus on and I would like you to address—I didn't come to just give a big speech—I would like you to actually address is, I think Americans have a reasonable expectation of privacy. But how do we define that? One of the things that I think we have to look at is airspace. It is reasonable that if somebody walked down your front yard, they could look at your front yard and see your mailbox and your shrubs and whatnot. As we expand out and start to use drones and satellites and other types of who knows what kind of technology, what is the reasonable expectation of privacy, say, in your backyard or on your private property?

And along with that is geolocation. I have sponsored a bill on this. I think it is going to continue to go on.

Would anybody care to address, what is the proper balance of airspace? You know, law enforcement use helicopters, right? We have allowed that for a long time; we think that is a good thing. But fuel is expensive. It is hard to get a helicopter. Law enforcement can only keep it up for so long. But if you have a drone that is up 24-7 or somebody that is going to—where is that balance? Where is that line?

Anybody care to take a stab at that one?

Mr. GRIMMELMANN. I can say a little bit about that.

One of the encouraging things about the Supreme Court's decision in *United States v. Jones* is that the Court endorsed two different kinds of rationales for protecting privacy.

One of them, based in the majority, is rooted in the historic law of trespass. And there, that might signal a reinvigoration of the idea that the airspace closely above your home is actually yours and not to be invaded. We have long accepted that commercial airlines can fly far overhead, but this might signal an attitude that we should protect your sovereignty over your own space close to the ground.

And the second, coming from the concurrences, is the so-called mosaic theory that continuous observation over a long period of time can ultimately build such a complete portrait that it does invade one's expectation of privacy.

Mr. CHAFFETZ. And I guess that is one of the challenges, Mr. Chairman, we face. Because he is right; in the Jones case, which is in large part what our legislation is modeled after, is this idea that there is a toggling between an individual's movements on private property and out in the public space.

Look, technology can be great. It can be so useful and make people's lives better. But how do we actually craft something without ruining the industry? That is the fundamental question.

I don't know if the other three care to jump in here.

Mr. REED. We have a phrase in the office. We say, "nobody wants technology at the speed of government." And that is the problem that the question that you point out raises.

You know, I speak as me, not as ACT. I would be totally creeped out having a drone fly above my house all the time, 24/7, watching my backyard. That is me; I am not speaking on behalf of our members.

But by the same token, a plane flying overhead isn't the problem. So we have to look at the behavior question, really. The plane flying overhead has an intent. It is going from point A to point B. It doesn't intend to be looking in my backyard. The drone positioned over my house watching everything that happened and whether or not I mowed the lawn on Sunday has the intent of watching what I am doing.

So I think that part of what—part of how we need to look at what technology empowers is, what is the intent of the person who is putting that technology in place? What do they want out of it? And that helps us guide the question of what is appropriate airspace in certain aspects that allows for wireless transmission to happen without impeding it with a lot of government regulation.

Mr. SHIPMAN. Yeah, if I could just add, I think, you know, the work that eBay and a number of other organizations have done in really framing what should Federal omnibus privacy law look like really focuses—and Mr. Reed used the word "intent"—it is use, it is use-based obligations.

With data, there is an intended use and there is an obligation that needs to come with that intended use. And you can look at each type of use: Is it fulfillment? Is it providing a service? Is it flying from point A to point B? And with that data collection and use comes obligation.

Mr. CHAFFETZ. Mr. Chairman, with all due respect—my time is well past gone—I would appreciate the industry continuing to look at this, because I think it is an incomplete answer. It is not sufficient enough to say that is the intent, because what does a celeb-

rity, for instance, in southern California do? You can see TMZ putting drones up trying to follow celebrities in their 10-mile zone—that is what "TMZ" stands for, right?—24-7.

So intent is not sufficient enough. I think the industry has also got to catch up on how to help us define that, because Congress has the ability to ruin people's lives, and I would rather not see that happen.

I yield back.

Mr. GOODLATTE. I thank the gentleman.

The gentlewoman from California, Ms. Lofgren, is recognized for 5 minutes.

Ms. LOFGREN. Thank you, Mr. Chairman.

And as Mr. Chaffetz has indicated, I have some reluctance to see Congress weigh in on these issues in a heavy regulatory manner because we don't work at Internet speed, we work at a different speed. And, you know, that is a good thing. I mean, we can't make mistakes quickly. But, certainly, the technology will move much faster than we can. And so I have been interested in how industry might establish standards that prevent a heavy regulatory load.

And along those lines, I am wondering how this process is working relative to the recent decision on Internet Explorer to make the default "do not track." I understand that there—and, certainly, Microsoft has the right to do that. Has that had an impact on the industry-wide effort to reach consensus on "do not track" or not?

Professor, could you answer that question?

Mr. GRIMMELMANN. So, the decision has been discussed within the working group that is building the standard. Some of the participants in that group, including representatives from Google, Yahoo, and Adobe, have taken the position that Internet Explorer should be defined to be noncompliant such that Web sites could say, I think you are using Internet Explorer, therefore I am not going to honor your "do not track" request. And I think this is simply an attempt to sabotage the standard. It won't work if Web sites can second-guess the user's statement, I don't want to be tracked.

Ms. LOFGREN. Well, the question, I guess, is for me, what is the default? What kind of transparency is available to the user? And, also, what kind of accountability is there if the user's choice is, in fact, not honored by the person representing the choice?

And I guess the question is, who owns this data? Maybe that is something that does need to be established in law, that the individual has an opportunity to enforce their own choices. Do you think that is an approach that would be helpful for Congress to take?

Mr. GRIMMELMANN. The default right now is that Web sites collect but offer the user an opportunity to opt out. I think users should have the opportunity to choose tools that protect their privacy by saying, "Do not collect," and if Web sites disagree with that choice, they can communicate with the user and say, "Here are the benefits we could offer you if you turned tracking on."

Ms. LOFGREN. Right. And that is—for example, I use Firefox. I don't know why, but I have always used it. And I have "do not track" turned on in my Firefox because that is a choice I want to make. But it means that there are some things I can't do on Firefox, which is a decision I have made.

Isn't it just—wouldn't it solve our problem in the Internet world if we were just transparent to users and gave them enforceable choices?

Mr. GRIMMELMANN. Yes.

Ms. LOFGREN. Now, let me ask about the—you know, Mr. Chaffetz, great minds think alike. I was also thinking about the drone issue. And I am told that in August the FAA is actually going to do some rulemaking on what drones can collect, which is kind of an odd regulatory role.

Recently, the FTC had a workshop on the use of facial recognition technology. Because this isn't just an online phenomenon. I mean, you go into every store in America, practically, and there is a camera that is taking pictures of the shoppers. And with facial recognition technology, you can now aggregate data about individuals, who they are. And, I mean, that is an immense amount of data that we I don't think have any rules about.

What are your thoughts on that?

Mr. REED. Well, the good news is that technology industries have actually been thinking on that. There are actually trade association efforts to develop best practices. And probably the best example I have seen to date on this is, strangely enough, Connect by Microsoft. They put together an incredibly comprehensive program prior to putting the Connect in your house. And you would say, well, why would that matter? But you realize, they are essentially facing a camera from the television at you. And so they did an entire privacy-by-design prior to launching Connect strictly on the question of facial recognition.

So the good news is smart people are starting the day saying, "how do we deal with this?"

Ms. LOFGREN. Well, but the issue is—and we have plenty of Fourth Amendment rules for the government, and that is important, I mean, obviously. But what we are talking about here is not the government but the private sector——

Mr. REED. Right.

Ms. LOFGREN [continuing]. Which we celebrate. I mean, the private sector is the job creator of our country, the engine of economic growth. And yet, the capacity to know everything about individuals because of technology that has been deployed, and yet individuals may not even be aware that their picture is being taken with facial recognition technology. They may have absolutely no privacy.

And I don't think we have any standards that are set for that use of big data. I mean, correct me if I am wrong.

Mr. SHIPMAN. No, actually, I think in that regard the online and mobile spaces are arguably doing a better job——

Ms. LOFGREN. Yes.

Mr. SHIPMAN [continuing]. At communicating what information is collected and how it is used. And I think that, as we see these technologies move into retail, that certainly companies like eBay that work with retail partners can form that partnership and can educate and help them with their use and their need to know their customer and how to balance that appropriately.

Ms. LOFGREN. I know my time is up, but I would just say that, you know, we need to have rules—individuals have to have the ability to enforce their understandings, either through the FTC or

through private rights of action. But we have not really looked at all to the non-online issues that may be even more severe than what people are paying attention to. Because everybody who goes online knows it is an issue. Nobody knows that the drone is in the sky or that the corner grocery is collecting their data.

Mr. REED. No, you are exactly right. And we all saw in the retail space that Target knew a young lady was pregnant before she had been able to tell her family. And that was not the online data collection at all; that was strictly from the retail store. So you are exactly right.

Ms. LOFGREN. Thank you, Mr. Chairman. My time is up.

Mr. GOODLATTE. I thank the gentlewoman.

The gentlewoman from Texas, Ms. Jackson Lee, is recognized for 5 minutes.

Ms. JACKSON LEE. I thank the Chairman very much.

And I thank all the witnesses for their testimony.

And I follow my colleague from California with the same quizzical concern about the extensiveness, the vastness of the issues dealing with Internet use and the concerns that we now have facing the American public or the world public. And so I want to raise some questions on that issue.

But before I do that, Mr. Reed, do you know the apps that are from Houston?

Mr. REED. I do. We have more than a few. From your district, we actually have—oh, there is a great app built by an African-American woman in your district who actually won the challenge grant from challenge.gov that helps people look up the average pay for the jobs they are applying for and helps them negotiate in their favor, because it tells them the public data, what the average rate of pay is. And it is an app, so you walk into your job interview and you know——

Ms. JACKSON LEE. And you are well-informed. Do you have some others that you can either refer us to or print out for us?

Mr. REED. Absolutely. But that one in particular was one that was really remarkable.

Ms. JACKSON LEE. It is remarkable and probably gives shockwaves to future employers. But I appreciate that.

Let me stay on the line of reasoning of my questions about privacy and use. Two examples. First, on the front page of the Web site CNET, there is a moving story of a paralyzed man who uses his eyes to tweet. This story demonstrates the enormous potential of the Internet.

How can this man be secure in knowing that when he uses a Web browser like Internet Explorer and chooses "do not track" that his instructions will be followed and not ignored?

Who wants to take that question? Professor?

Mr. GRIMMELMANN. The important part there is that once "do not track" is standardized, I hope that Congress and the FTC will see fit to treat that as an enforceable practice, either under the principles of contract law or as a deceptive trade practice. A consumer's request not to be tracked should be honored.

Ms. JACKSON LEE. And how long—or what should we do to move that standardization forward in terms of the industry, to move forward on the standardized practice?

Mr. GRIMMELMANN. Fortunately, the working group that is discussing it has an active and aggressive schedule. As long as they are aware that Washington is watching and hoping for them to succeed and waiting for the results, I think that is the most important thing you can do now.

Ms. JACKSON LEE. So you would say contract law, and what would be the other enforcement?

Mr. GRIMMELMANN. The FTC's ability to prohibit unfair and deceptive trade practices.

Ms. JACKSON LEE. And my concern would be, what are we doing now? But I appreciate what you are saying is that we are on the right track.

Let me also add this question. I appeared this morning discussing another topic, which is immigration reform, on C-SPAN, but a question was raised before I came on. In a Google official report by Dr. Dorothy Chou on the alarming number of requests for government censorship, the United States was number one.

But the question is, the government has a special role and responsibility. What should Congress' role be in monitoring, permitting or opposing censorship by the government? I will go to the professor, but I would like some others to chip in.

Mr. GRIMMELMANN. So, law enforcement requests come from a wide variety of sources, government both in the United States and abroad. And so the role of Congress there is, in part, to monitor the requests coming from the United States entities and, in part, also to work with U.S. companies over the pressure they are receiving from foreign governments to censor and to help give them the protection and reassurance of the United States Government that we support free expression around the world.

Ms. JACKSON LEE. But are you saying we make statements? I mean, because it is—we are asking to protect what we are transmitting. So the point is that the government is making these points that they need to, in essence, protect what they have.

Mr. GRIMMELMANN. There was a conversation that has been going on for a number of years over global Internet freedom principles, and part of that is in a discussion about possibly legislating responsibilities for United States companies to be transparent about their degree of compliance or resistance to foreign censorship attempts. Google's transparency about requests it receives was actually quite helpful in understanding the pressure that governments put on our companies to do their dirty work.

Ms. JACKSON LEE. I think that is a very sensitive question that is appropriate for a congressional review.

Let me go to Mr. Babel to talk of the challenges of privacy as you established your company.

Mr. BABEL. Sure. The challenges are really in helping companies and consumers kind of meet that best practice of where there is trust by consumers that the companies are doing the right thing. So our kind of sole role for existence is helping clients, customers understand what best practices around privacy really are and helping them prove to consumers that they are doing the right thing with their, you know, personal information. So that is what TRUSTe is really there in helping the ecosystem know and under-

stand and balance that trust relationship between business and entities.

Ms. JACKSON LEE. Are your customers bankers or banks?

Mr. BABEL. There are a few banks, but it is really more focused on more online companies and technology companies. And we assist banks with other regulations that they have.

Mr. GOODLATTE. Thank you. The time of the gentlewoman has expired.

Ms. JACKSON LEE. I yield back.

Mr. GOODLATTE. The gentleman from Georgia is recognized for 5 minutes, Mr. Johnson.

Mr. JOHNSON. Thank you, Mr. Chairman.

And I must admit that I was just a little disturbed, Mr. Reed, when you kind of left me out of the equation. I am sitting here right in front of you, closest to you; we could almost breathe on each other. And you didn't mention any apps from——

Mr. REED. I can talk about your app. It is good. I will give you it right now. It is a great app that allows you to pay for your parking spot with your mobile phone. It is actually one that a lot of us already use. It is called Parkmobile. It is a great app. Lets you pay for parking with your mobile phone. There you go.

Mr. JOHNSON. Oh, I tell you, thank you.

I also found one from Decatur, which is where I represent, Ping, a subsidiary of Ping Media Group, Incorporated. It is a provider of mobile coupons and promotions which enable retailers and vendors to communicate directly with their customers via mobile phones.

And then I got another one. A young man, 17 years old, his name is Albert Renshaw, out of Gwinnett County, which I also represent. He has developed Apps4Life—A-P-P-S-4, the number, L-I-F-E—which offers WiFi texting without a wireless connection. And I thought those were pretty good.

But I will now get into the meat of my concern. A breach in security protocol by a company such as eBay that exposes private customer information to the public could result in death or grievous bodily injury to a customer whose private information was divulged wrongfully. The consumer certainly has a right to recover damages for his or her injury, or their next of kin for their death. I am sure you all would not disagree with that. And they have a right to seek a recovery in a court of law. But one of the—and that is one of a consumer's basic rights.

But that right is being chipped away at with these mandatory pre-dispute arbitration—mandatory arbitration clauses in these consumer agreements, which prohibit the individual, the aggrieved party, from being able to sue in court. Instead, they are forced into mandatory arbitration where the arbitrator is selected by the company. The arbitrator may or may not be a lawyer. The arbitrator does not operate in a public courtroom, but it is a private, secret proceeding, maybe held miles away, hundreds and thousands of miles away, from where the aggrieved party actually lives.

There are no rules of Federal procedure, rules of civil procedure, rules of evidence, and no jury trial. You know, the arbitrator decides the issue, and then once the arbitrator does, there is no right to an appeal. This is a private system of adjudicating disputes

which consumers sign up for a consumer agreement without any knowledge of the gravity of what they are giving up.

Mr. Shipman, what do you think about that? Does your company have to sue sometimes other competitors for various things in a court of law? And do you think that it is important that consumers have the right to take their matter to court as well?

Mr. SHIPMAN. So, certainly the scenario you paint is an awful and terrible scenario for that family and one that I would hope that we never encounter.

I think there are two important points here. The first is, what are the terms that the company has with a customer? And——

Mr. JOHNSON. What does?

Mr. SHIPMAN. What are the terms. Is there an arbitration provision or not.

Mr. JOHNSON. Yeah.

Mr. SHIPMAN. And——

Mr. JOHNSON. Do you know whether or not you have that in eBay?

Mr. SHIPMAN. In the case of eBay, we actually have a number of choices for our customers, depending on the size of the claim. If it is a financial-related claim, it may be available to small claims action. If it is a larger claim, then certainly you can bring that case. We don't have that arbitration provision that would prevent someone from being able to be heard and, you know, have their day in court.

The second theme that you talk about is information security and the protection of information. And, certainly, you know, a responsible company has thousands of people devoted to making sure that the information that is entrusted with us is taken care of appropriately. Because the last thing we want, certainly, is that scenario that you paint, because that is awful for not only our business but also for our customers.

Mr. JOHNSON. Well, certainly. And it is not that the company would intend for any harm to come to one of its customers because of a breach. It could happen, though, pretty easily given the fact that this marketplace is in its earliest stage of development and growth and mistakes can be made along the way with various applications. Something may have a bug that needs to be worked out. And it is definitely possible for someone—let's say, a woman whose husband or boyfriend, you know, wants to do some damage to them and, due to a breach of information, is able to follow through with that, either, you know, character-wise or reputation-wise or either coming to the house and cutting her up into a million pieces. You know, it could happen.

And if it does happen, then if eBay decides that, okay, this claim is not worth that much, then it will go through a certain procedure, and if it is deemed by eBay to be larger than that, then it goes into—then the person has a right to go to court. Is that what we are talking about?

Mr. SHIPMAN. Well, you know, again, I mean, very awful scenarios that you are painting. But——

Mr. JOHNSON. But, I mean, it is true. Anything might happen.

Mr. SHIPMAN. Nonetheless—and, certainly, we can follow up with you afterwards. We would love to work with you.

You know, our clause allows consumers to decide what the remedy—you know, what avenue they have available to them. We don't limit all claims to arbitration. So I think that is, you know, the salient piece.

Mr. JOHNSON. Okay.

Mr. SHIPMAN. The second thing is, on this issue of a security breach, what we have seen to date—and I can't summarize and you don't want me to summarize all of the legislation and the caselaw—but what we have seen to date is, where there is a harm—and in the cases that you are providing, there are clear harms—then it is likely, I believe, that you would see damages be appropriate. Where we have seen no harm—no financial identity theft, no physical harm—the cases that we have seen generally tend to say that there is not liability in that regard.

Mr. JOHNSON. I understand.

Professor Grimmelmann, your response, sir, or insight?

Mr. GRIMMELMANN. I agree with him that where there is physical harm to the individual who has been hurt as a result of the breach, then, yes, the courts are available, and they have been willing to hear those suits.

I am concerned somewhat that the breaches that do not result in immediate provable harm but nonetheless reduce the information security for all of us by leaking financial information on many consumers that can lead to acts of identity theft that can't specifically be tracked back to that one individual breach have resulted in harm not provable in a court of law, and so, therefore, there is no redress against it.

This is why data-breach notification laws and other efforts to shine a light on this and enforce basic information security practices against industry participants are important.

Mr. JOHNSON. Uh-huh. Class action litigation could play a part in deterring willful misconduct that could ensue.

Mr. GOODLATTE. The time of the gentleman has expired.

Mr. JOHNSON. I noticed that red button has been on ever since I started talking, so I don't know how long I have gone, Mr. Chairman. But it doesn't seem like 5 minutes, though.

Mr. GOODLATTE. Without objection, the gentleman will be recognized for 1 additional minute to sum up his ideas.

Mr. JOHNSON. Thank you.

Yeah, class action litigation, where a number of people have suffered just a small amount of harm, but the class action litigation, which can result in a verdict of some importance in terms of the amount, could act as a deterrent and is good for public policy, in my opinion.

What would be your response to that, Professor Grimmelmann? Because I don't want to—I don't want to personalize this with eBay. eBay is no different than all of the other entities out there that are very popular with consumers. So I will ask you, Professor.

Well, I will ask Mr. Reed. What do you think?

Mr. GRIMMELMANN. This is an area——

Mr. JOHNSON. Go ahead. Go ahead.

Mr. GRIMMELMANN. This is an area in which you are concerned about arbitration, which is extremely important, and this is also an area in which class-action litigation has been important for privacy.

Facebook has recently settled a lawsuit over its marketing a commercial product using individuals' pictures to say, "James just watched 'WALL-E.' Don't you want to watch it, too?" to their friends. And a class-action lawsuit resulted in a $10 million settlement.

Mr. JOHNSON. Thank you.

Mr. GOODLATTE. The time of the gentleman has expired again.

Mr. JOHNSON. Thank you, Mr. Chairman.

Mr. GOODLATTE. And having allotted him 10½ minutes on his 5 minutes of time, I am going to take the privilege of asking a clarifying question for the witnesses.

To me, self-regulation means companies publish their policies, and then if they engage in deceptive practices by not following those policies, then under existing law the Federal Trade Commission would have the authority to take action for false advertising or whatever the case might be.

What I want to know for sure here is, does anyone here believe that the Federal Government should impose a one-size-fits-all regulatory approach or that the Federal Government should proscribe specific privacy policies to specific companies or in general?

Mr. Shipman?

Mr. SHIPMAN. No, I don't think the government should draft specific privacy policies. I think we should leave that to industry and those that are innovating the services and technology.

Mr. GOODLATTE. Thank you.

Mr. Reed?

Mr. REED. Exactly the same. I agree completely. That is not the position the government should be in.

Mr. GOODLATTE. Mr. Babel?

Mr. BABEL. I would agree, and also agree with your view that self-regulation with, kind of, a proper backdrop with the FTC is a good program to continue.

Mr. GOODLATTE. Mr. Grimmelmann?

Mr. GRIMMELMANN. I agree that government should not regulate specific privacy policies. It should make sure that consumers have effective notice of what those policies are and have enforcement when those promises are broken.

Mr. GOODLATTE. Thank you very much. That definitely is clarifying information from all of you.

I would like to thank all of our witnesses for their testimony today. This has been a very informative hearing.

And, without objection, all Members will have 5 legislative days to submit to the Chair additional written questions for the witnesses, which we will forward and ask the witnesses to respond as promptly as they can so that their answers may be made part of the record.

And, without objection, all Members will have 5 legislative days to submit any additional materials for inclusion in the record.

And, with that, I again thank all of our distinguished witnesses.

And the hearing is adjourned.

[Whereupon, at 12:02 p.m., the Subcommittee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record

Response to Post-Hearing Questions from Scott R. Shipman, Associate General Counsel, Global Privacy Leader, eBay Inc.

Question Offered by Representative Judy Chu:

As you most likely know, Microsoft recently made an announcement that its Windows 8 will include an Internet Explorer that will have a Do Not Track feature that defaults to "on," which will require consumers to actively opt-in to targeted adversity. Many in the online ad industry believe Microsoft's announcement can potentially upend much of the work that industry was doing to self-regulate online behavioral advertising. However, I read in your testimony that eBay Inc. has done something similar and has made it a standard practice that all consumers opt-in to turn on geo-location for all of eBay Inc. mobile applications. Given eBay's commitment to continuing and respecting privacy, what are your thoughts on Microsoft's Do Not Track announcement?

Scott Shipman Response:

Congresswoman Chu, thank you for your question and for your interest in this important issue. As I stated during my testimony, eBay is committed to meeting customer privacy expectations with every product we offer and we strive to treat our users' data with the utmost respect.

You asked me for my specific thoughts regarding Microsoft's recent Do Not Track Announcement. Unfortunately, I cannot speak to the privacy practices of other companies and can only speak to the privacy principles that eBay has adopted across our family of companies. And as a company, we developed and implemented a program in 2007 called AdChoice, which was the first choice mechanism that offered consumers the ability to express their preferences for how their data was used for behaviorally targeted advertising We recognized early on that a mechanism was needed to provide consumers with more meaningful choices and control over the way their aggregate anonymous data was used for behaviorally targeted advertising purposes. Since then, a group of major marketing and media companies launched a similar program, which endorsed the use of the "Advertising Option Icon."

In addition, it is important to note eBay supports policymakers' efforts to encourage greater consumer choice and control and we believe that the development and universal implementation of baseline choice mechanisms would be a step in the right direction to address the concerns that have been expressed regarding behavioral tracking and advertising.

Furthermore, it is our belief that each entity should have the ability to offer a mechanism that best fits their business model or the needs of their users. Choice mechanisms could

include anything from customized web-based solutions, a centralized opt-out website for participating members, third party add-ons, or a solution integrated within a browser. However, eBay does strongly caution policymakers from adopting or promoting a singular technological approach to this issue. Creating a one-size fits all standard will only hinder the continued growth of the ecommerce industry. In addition, there are commonly accepted business practices that employ tracking that could get swept up into the Do Not Track technology, leaving some businesses very vulnerable. For instance, there is a certain level of tracking that needs to occur in order for a company to protect itself against fraud or other illegal activities.

In addition, it is important to distinguish between 1st party and 3rd party tracking and use. It is critical that we do not needlessly interfere in an arm's length relationship between a consumer and the company. By limiting 1st party tracking, policymakers could be restricting the sharing of legitimate customer information that is necessary to fulfill the service that the consumer has requested and expects to receive from the company.

Again, I sincerely appreciate your question and would be happy to provide further clarification to you and your staff on this issue or any issue related to privacy and consumer protection. Thank you for the opportunity to testify before the Committee on this important issue and we look forward to working with you in the future.

Response to Post-Hearing Questions from Chris Babel, Chief Executive Officer, TRUSTe

July 23, 2012

Representative Bob Goodlatte
Chair, Committee on Judicary
Subcommittee on Intellectual Property, Competition & the Internet
U.S. House of Representatives
2138 Rayburn House Office Building
Washington, DC 20515

Via email: Olivia.lee@mail.house.gov

Re: Questions for the Record for hearing on "New Technologies in the Mobile and Online Space & the Implications for Public Policy," June 19, 2012

Dear Rep. Goodlatte:

Thank you for your letter dated July 9th, 2012. I appreciated the opportunity to testify at the June 19th hearing and hope that you found my testimony useful.

Following up from that correspondence, here are my answers in response to Representative Chu's questions:

1. **In your testimony you referenced a survey that found that "85 percent of consumers want to be able to opt-in or out of targeted mobile ads." Given this finding, do you think that consumers would prefer the approach recently announced by Microsoft, which defaults to an opt-in system, or the self-regulatory approaches by many in the ad network industry that allow consumers to opt-out?**

At TRUSTe we believe privacy is best served when consumers are informed and have the ability to indicate their preference for how a business uses their data. Our research[1] shows that while online behavioral advertising across platforms (including mobile) remains a privacy concern, a majority of consumers believe that they themselves are most responsible to make decisions about safeguarding their privacy online. This means that preserving consumer choice must be an important consideration for any online product or service. Unlike security, where things like encryption are universally better for a consumer and therefore should be pre-configured on their behalf, privacy is highly contextual and defined in part by social norms. Something that is perfectly acceptable to one individual may be completely abhorrent to another. This is especially true of online behavioral advertising; while some consumers like the idea of receiving ads that are targeted to their interests, others find the practice particularly invasive.

[1] 2011 privacy study with Harris Interactive

We commend Microsoft's efforts to build privacy into their products[2]. Historically, default privacy settings, irrespective of browser provider, have not specified thorough robust notice or similar mechanisms whether the setting is defaulted to opt-in or opt-out. TRUSTe believes that it is important for consumers to understand their browser settings and know how they can use these settings to make privacy choices. The current unknown in the Microsoft approach is that they have not shared the design and flow of the user experience so it is very difficult to understand how the user will be notified of this default setting and be prompted to manage their preferences. Given the highly contextual nature of privacy, the decision on how a consumer will experience the web in terms of the ads they choose to receive is something that the individual consumer should get to decide for his or herself. Microsoft will be testing the impact of the default-on Do Not Track ("DNT") setting in Internet Explorer and collecting consumer feedback in response and we look forward to learning more about these details.

In addition, TRUSTe's research[3] shows that a large number of consumers see other stakeholders – including ad networks, browser manufacturers, government, independent privacy organizations, social networks, and website publishers – as also being responsible for safeguarding privacy online. Thus, when it comes to online behavioral advertising and tracking, we believe consumers prefer a self-regulatory approach that inherently involves the participation of a wide range of stakeholders and preserves the consumers' right to choose. TRUSTe is actively participating in a broad stakeholder effort around tracking - the W3C Tracking Protection Working Group. We believe that this effort provides the best hope for a DNT standard that works for consumers, government and the wide range of industries that populate the online ecosystem.

Consumer education also plays an important role here. While overall industry investment in consumer tools and education has not kept pace with advances in online tracking practices over the past decade, several new programs have rolled out in the past 18 months that are starting to address this gap. These include the DAA Ad Choices self-regulatory program, as well as TRUSTe's consent management solutions that address compliance with the EU Cookie Directive and provide users with a specific tool to manage their cookie preferences.

2. **Proponents of a self-regulatory framework for monitoring or addressing online privacy practices assert that self-regulation is preferable for many reasons, including that such a mechanism provides incentives for compliance. However, I**

[2] Microsoft is a current TRUSTe client
[3] 2011 privacy study with Harris Interactive

would like to look at this issue from a consumer perspective. Why should a consumer trust online companies to protect their privacy through a self-regulatory framework rather than looking to Congress to provide assurance that their data will be protected and secured?

As mentioned above in Answer 1, consumers view themselves as most responsible to make decisions about safeguarding their privacy online along with other stakeholders like ad networks, browsers, government, independent privacy organizations, social networks and website publishers.

We believe that a self-regulatory framework based on established principles and best practices, and forged through industry consensus, is best equipped to protect consumers' privacy online. Not only can self-regulation address rapidly changing business practices in dynamic industries like technology, a good self-regulatory program also incorporates feedback from consumers, and recognizes the importance of education to help consumers make informed decisions about the privacy choices available to them.

We also believe that self-regulation should work in tandem with regulatory enforcement so long as the self regulatory program includes protections like a safe harbor and due process as described in our written testimony. We support the Federal Trade Commission's authority under Section 5 to protect consumers against unfair and deceptive trade practices especially in cases where companies willfully disobey self-regulatory requirements to the detriment of consumers. We think that regulatory enforcement under existing law helps keep the market competitive for privacy focused businesses, while also protecting consumers from bad actors.

Please let me know if there's any additional information I can provide either in response to Representative Chu's questions or with regards to my testimony.

Sincerely,

Chris Babel
CEO

Response to Post-Hearing Questions from James Grimmelmann, Associate Professor of Law, New York Law School

Hearing on: "New Technologies and Innovations in the Mobile and Online space, and the Implications for Public Policy"

Tuesday, June 19, 2012

Question Offered by Representative Judy Chu:

What are your thoughts on Microsoft's recent announcement of Do Not Track for Internet Explorer 10? Do you believe that a privacy-by-default state for online behavioral advertising is the right approach? If so, why?

Response from Professor James Grimmelmann:

I thank the Subcommittee and Representative Chu for the opportunity to answer this follow-up question.

Microsoft's decision to enable the Do Not Track header by default in Internet Explorer 10 is a valuable innovation. As I stated in my testimony before the Subcommittee, it is important that privacy choices be usable by consumers. Unnecessarily complicated interfaces can confuse users in ways that cause them to make mistakes and undercut their privacy. A default has the virtue of being inherently usable: anyone who able to use Internet Explorer is able to use its Do Not Track setting. Users who are concerned by how much websites know about them do not need to understand the details to take a simple step to protect themselves.

Thus, I consider Internet Explorer's decision to activate the Do Not Track header by default to be an example of innovation for privacy in action. It is impractical, indeed impossible, for users to make specific privacy choices about every last detail of their online activities. Browser vendors compete to offer users a good combination of privacy and usability. Like the third-party cookie blocker in Apple's Safari or Chrome's integrated protection against sites known to be distributing malware, Internet Explorer's Do Not Track default setting is a useful innovation that some users may find helpful. Users who dislike the setting can easily change it, or use a different browser.

A slightly different question is whether Congress should mandate a default against tracking for all browsers and websites, not just Internet Explorer and those that choose to honor the Do Not Track header. As I stated in my testimony at the hearing, I believe that Congress's most appropriate role at the moment is to observe and encourage the World Wide Web Consortium's consensus process to develop a technical standard for expressing tracking preferences and an agreed-upon definition of "tracking." If that process results in an outcome in which websites and advertisers honor the Do Not Track header when they observe it, further action may be unnecessary. But if the process fails to reach consensus, the resulting standard does not accurately reflect users' understandings of tracking, or if Do Not Track requests are widely ignored by websites, it would be appropriate for Congress to legislate a baseline permitting tracking for behavioral advertising only on an opt-in basis.

Prepared Statement of the Consumer Electronics Association (CEA)

Before the
Subcommittee on Intellectual Property, Competition and the Internet
Committee on Judiciary Committee
U.S. House of Representatives

Hearing on "New Technologies and Innovations in the Mobile and Online Space, and the Implications for Public Policy"

Statement of the
Consumer Electronics Association (CEA)

June 19, 2012

Subcommittee Chairman Goodlatte, Ranking Member Watt and Members of the committee, on behalf of the Consumer Electronics Association (CEA), thank you for the opportunity to submit written testimony for today's hearing on new technologies and innovations in the mobile and online space.

CEA is the preeminent trade association representing the consumer technology industry. CEA's over 2,000 American corporate members include manufacturers, internet providers and retailers. Our members design, produce and sell the exciting products and provide the essential services that enable millions upon millions of consumers every day to access the wonders of the Internet. We own and produce the world's most important technology event, the International CES. In May, CEA hosted its annual "CES on the Hill" in the Rayburn Building to demonstrate a fraction of products with policy implications to lawmakers like you. Tonight, CEA is sponsoring the "Startup The Hill" reception in HC-5 in the Capitol from 6:00 to 7:30 pm, which features a number of small startup companies, which are on the frontlines of innovation. We hope you will consider stopping by this exciting event.

Even in these troubling economic times, the technology industry's direct contribution to the American economy is remarkable. Today, the consumer electronics sector directly and indirectly generates $1.4 trillion in output, $325 billion in salaries, $145 billion in tax payments, and 4.4 million jobs in the United States. This economic activity translates into a contribution of $585 billion by the CE sector to U.S. gross domestic product ("GDP") — 4.6 percent of the entire national economy. More, our industry is a vital link in supporting the fast growing ecommerce economy.

Thus, as a matter of national economic policy, we ask that Congress support growth and innovation in the consumer technology sector. As part of a pro-innovation strategy, CEA advocates for a shift to strategic immigration: policies to attract the best and the brightest to come to the United States and stay and build businesses here. CEA supports policies that would: reform the H1B visa program so that foreign graduates of U.S. schools can become American entrepreneurs and fuel innovation and economic growth in our country, not abroad; allow a quick path to citizenship for entrepreneurs; and create criteria and a process for granting citizenship to qualified immigrants. This is a public policy issue that the Judiciary Committee has clear jurisdiction over and it is our sincere hope that the Committee will soon consider legislation that embraces these policies.

For any public policy favoring growth and innovation, any policy should first do no harm. Despite overwhelming evidence of ever-increasing Internet use by the America public and its attendant economic growth, we are concerned that Congress will only heed those who clamor for government action which could fundamentally reshape the mechanics of how the internet functions and how the delivery of free online content works. We suspect that the medicine may be worse than any disease and urge a healthy dose of free market skepticism towards those alleging that consumer online trust or

confidence is somehow lacking and increased government protections are essential to sustaining and augmenting it.

CEA member companies almost all have valuable brands in which they have invested. Preserving a brand means not allowing your reputation to be sullied by breaching trust with your consumers and the public. Most companies believe that respect for consumer privacy is an important and vital business practice. Our member companies are committed to being responsible data custodians. They have and continue to develop, implement and enforce robust practices, based on industry self-regulation. They apply best business practices in a variety of areas related to consumer privacy. Our members believe that any policy proposals concerning privacy and electronic data collection should be based on a set of core principles as follows:

The primary goal of any legislation or regulation concerning online privacy issues should be to enhance individuals' continued use of and trust in technology and technology products;

Privacy legislation and regulations must be technology-neutral; that is, no one particular solution should be mandated nor should technology products be burdened with providing the sole resolution;

The definition of harm resulting from the use of consumer data collected electronically should be agreed to, including its standard of proof, before any overarching privacy legislation and/or regulations are adopted;

International agreements, such as the US-EU Safe Harbor framework, must be maintained so that U.S. companies have a streamlined means to comply with the EU's "adequacy" standard for privacy protection;

Innovations in technology and resulting consumer benefits made possible through electronic data collection should be protected and promoted. Efforts should be made to increase consumer knowledge about existing privacy protections, as well as the benefits to consumers made possible through electronic data collection; and

Self-regulatory approaches to privacy protection should be encouraged and embraced.

CEA calls for targeted government action if and when the data clearly indicates the need for a public policy solution. We support established privacy laws and regulations in the identity theft, health care and child safety sectors because of the evident harm to consumers if their information is misused or without their consent. But we find the evidence lacking regarding the alleged harm to consumers that some now seek to mitigate.

Before any solution is adopted, we must first collectively come to a definitive, clear and data-based conclusion and consensus about what issue, if any, we seek to solve. CEA takes the position, as noted in our fifth privacy principle, that data collected electronically provides enormous consumer benefits and services. As such, we believe that any discussion of the supposed harm must also be measured alongside the advantages afforded by the rich and often-times free innovations available online.

CEA, on behalf of its over 2,000 member companies, stands ready to serve Congress and the Administration as a participant and resource on the topic of privacy and other issues related to supporting innovation.

○