S. HRG. 112–289

CONSUMER PRIVACY AND PROTECTION IN THE MOBILE MARKETPLACE

HEARING

BEFORE THE

SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, AND INSURANCE

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

MAY 19, 2011

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

U.S. GOVERNMENT PRINTING OFFICE
73–133 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

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

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

DANIEL K. INOUYE, Hawaii	KAY BAILEY HUTCHISON, Texas, *Ranking*
JOHN F. KERRY, Massachusetts	OLYMPIA J. SNOWE, Maine
BARBARA BOXER, California	JIM DEMINT, South Carolina
BILL NELSON, Florida	JOHN THUNE, South Dakota
MARIA CANTWELL, Washington	ROGER F. WICKER, Mississippi
FRANK R. LAUTENBERG, New Jersey	JOHNNY ISAKSON, Georgia
MARK PRYOR, Arkansas	ROY BLUNT, Missouri
CLAIRE MCCASKILL, Missouri	JOHN BOOZMAN, Arkansas
AMY KLOBUCHAR, Minnesota	PATRICK J. TOOMEY, Pennsylvania
TOM UDALL, New Mexico	MARCO RUBIO, Florida
MARK WARNER, Virginia	KELLY AYOTTE, New Hampshire
MARK BEGICH, Alaska	DEAN KELLER, Nevada

ELLEN L. DONESKI, *Staff Director*
JAMES REID, *Deputy Staff Director*
BRUCE H. ANDREWS, *General Counsel*
BRIAN M. HENDRICKS, *Republican Staff Director and General Counsel*
TODD BERTOSON, *Republican Deputy Staff Director*
REBECCA SEIDEL, *Republican Chief Counsel*

SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, AND INSURANCE

MARK PRYOR, Arkansas, *Chairman*	ROGER F. WICKER, Mississippi, *Ranking*
JOHN F. KERRY, Massachusetts	JOHN ENSIGN, Nevada
BARBARA BOXER, California	JOHN THUNE, South Dakota
CLAIRE MCCASKILL, Missouri	JOHN BOOZMAN, Arkansas
AMY KLOBUCHAR, Minnesota	PATRICK J. TOOMEY, Pennsylvania
TOM UDALL, New Mexico	

CONTENTS

CONSUMER PRIVACY AND PROTECTION IN THE MOBILE MARKETPLACE

THURSDAY, MAY 19, 2011

U.S. SENATE,
SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, AND INSURANCE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10 a.m., in room SR–253, Russell Senate Office Building, Hon. Mark Pryor, Chairman of the Subcommittee, presiding.

OPENING STATEMENT OF HON. MARK PRYOR, U.S. SENATOR FROM ARKANSAS

Senator PRYOR. I will go ahead and call our subcommittee to order here. I want to thank everyone for being here. We have a standing room only crowd.

I want to welcome Senator Toomey, who is just sitting down here, as the new Ranking Member. Welcome aboard. We are excited about you and your leadership here. And you and I need to talk offline at some point about this great subcommittee, but thank you for being here.

And Senator Kerry, thank you for being here.

We have others that are on the way, but I would like to go ahead and start. I know that Senator Kerry only has a limited time here, and my understanding is Senator Rockefeller is trying to make it, and he has limited time. So let us get under way.

I would like to welcome everyone, thank everyone for being here, thank all of our witnesses who are participating today. Certainly, this is a very important hearing on privacy in the mobile marketplace. As Chairman of the Consumer Protection Subcommittee, I appreciate all of your willingness to participate in this very important dialogue.

As technology evolves, consumers continue to lose control of their personal information. Without question, cell phones have become a part of that trend, as they have become more and more versatile. Today, more than 234 million Americans use mobile devices, and 73 million Americans have smartphones or are expected to own smartphones by the end of 2011.

There are hundreds of thousands of software applications, also known as apps, on the market today. Apps allow us to play games, share information with friends, read the news, find the cheapest gas in town. In fact, I am aware of one app that allows people to

find the nearest kosher restaurant and nearest synagogue. So there seems to be an app for everything.

And while their innovation and creativity has defined the mobile app space, we understand that most of the app producers do not have a privacy policy. And the vast majority of consumers who use these apps really don't have any idea about the ways their personal information—including their age, location, gender, income, and ethnicity—that is contained in their phones can be shared either with the company or with third parties.

In other words, while smartphone users may voluntarily submit some information to software applications, it is not clear that Americans who own smartphones understand how their information may be used or transferred as a result of the download.

In fact, last night I talked to my two teenage children. Both of them have apps that share information. Neither of them had any idea that that information was being shared, and I think that is the way most Americans are.

Consequently, it is not surprising that we are facing a new and emerging mobile world that lacks basic parameters and best practices. Where are the opt-out options or where are the privacy policies? And that is some of the things we will talk about today.

The mapping of consumers' movements without consent is unacceptable, and an application game that transfers a consumer's location data to ad networks without informing the user is greatly troubling. While location technology can assist law enforcement, and there certainly are good things about it—it can be helpful in emergency situations—geolocation tracking also poses serious safety concerns.

Therapists who work with domestic abuse victims have noted the increase in clients stalked via cell phones. Indeed, a *Wall Street Journal* article cited tragic instances where stalkers exploited the GPS system and the location data collected by consumers' smartphones to track their victims. The results have been deadly in some cases.

Demonstrating the highly intrusive nature of some of this technology, one website sells something they call "Mobile Spy" software and actually markets this product as a completely stealth monitoring program. The website says once installed on a phone, Mobile Spy remains hidden, but logs calls and text to a Mobile Spy server. Then the snoop can log in and see a complete record of incoming and outgoing calls, the time and duration of the calls, and read text messages, both sent and received.

So I would like to hear from our witnesses today about the risk to consumers, that consumers see when their information is collected and reported; the consumers' understanding of what information is being collected or transferred through mobile apps; the extent of geolocation information collection and related privacy concerns, particularly with an emphasis on children there; how companies are working to allay these concerns; and suggestions for enforcement of basic privacy rights and security policies and standards in the new app economy and online mobile world.

So, with that, what I would like to do is turn it over to the Ranking Member and allow you to say a few words. Then we will call on Senator Kerry.

STATEMENT OF HON. PATRICK J. TOOMEY,
U.S. SENATOR FROM PENNSYLVANIA

Senator TOOMEY. Senator Pryor, Mr. Chairman, thank you very much.

First of all, thanks for welcoming me as the new Ranking Member on the Subcommittee. This is a new and exciting opportunity for me. I am looking forward to serving with you.

And I also want to thank you for scheduling this important hearing. This is a very important topic, and I commend you for doing that.

Unfortunately, I became Ranking Member just in the last couple of days and, prior to that, had a previously scheduled conflict. So I won't be able to stay, but I did want to make an opening statement, if I could, quickly and again commend you for doing this.

Like most Americans, I am protective of my personal information, and I believe I should have control over who accesses that information, how it is accessed, and ultimately, how it is used, including by commercial entities.

As the father of young children, I am also very concerned about protecting their identity and safety, especially when they use mobile devices and other online applications. More children are accessing online services through home computers and mobile devices than ever before, and ensuring that parents are well informed on how best to protect their children is a goal that I am sure we all share.

Recent revelations that Apple iPhones have been tracking and storing user locations without consent and Facebook apps may have leaked profile information to advertisers are certainly causes for concern. These and other incidents have led many in Congress to question whether the Federal Government may have a legitimate interest in increasing its role in regulating this space.

I do, however, want to commend Apple and Facebook for taking swift action in both cases to correct the problem. As a general matter, I prefer to see the industry self-regulate, and I am eager to learn from our witnesses on the measures that have been put in place to safeguard against possible future consumer harms.

I think everyone here knows very well the mobile marketplace is growing and changing rapidly. We now have access to mobile devices, speeds, and applications that were completely unimaginable just a few short years ago. Apps for smartphones have quickly turned into a multibillion-dollar business, and consumer demand is clearly very strong.

And in our important efforts to protect consumer privacy, I just hope that we won't lose sight of the many consumer benefits that have come from the innovative technologies that are brought to market by the companies that we will be hearing from today.

As the Chairman indicated in his comments, location-based services provide conveniences that consumers wouldn't have if a particular app didn't have access to some level of personal information. So before Congress takes action, I think it is important to find the right balance that protects consumers' personal information while, at the same time, allows continuing constructive innovation to occur.

At this point, I am not quite sure exactly where that line is to be drawn, and I would caution against passing legislation that would have unintended consequences. I am hopeful that the hearing today will shed some light on this important question.

And again, Mr. Chairman, I thank you for scheduling the hearing.

Senator PRYOR. Thank you very much.

And we also want to thank our newest member to the Subcommittee and to the Committee and to the Senate. Senator Heller, thank you for being here. Proud to have you.

Now, I was going to call on Senator Kerry. And the Chairman says I should call on Senator Kerry. So go ahead.

STATEMENT OF HON. JOHN F. KERRY,
U.S. SENATOR FROM MASSACHUSETTS

Senator KERRY. Well, thank you. Thank you. Thank you, both chairmen.

And welcome to our new members on the Committee.

Mr. Chairman, thanks for holding this hearing today. It is obviously one that attracts a lot of interest. It is a lot of money on the line, a lot of business, a lot of business practices, but also a lot of values, personal interests of Americans.

And while today's hearing is, obviously, principally about mobile phones and the apps that come with them, which are quite extraordinary and which we all use and benefit from in a lot of ways, it is also important, I think, to put the mobile phone and apps in the context of the larger discussion about privacy itself.

I don't think there is anybody on the Committee or in the country or in the world who doesn't marvel at the power and the extraordinary potential that we are currently living and that we will live in the future with respect to the Internet. It is constantly innovating and moving, and I am personally—and I know the Chairman, Senator Rockefeller, likewise and a bunch of us on the Committee have worked hard and long with respect to the National Broadband Plan, as well as the issue of releasing more spectrum for broadband because we want to see this potential of the Internet unleashed all across the country as broadly as possible.

In fact, we have, unfortunately, in the United States of America parenthetically, been going in the wrong direction. We used to be number four in the world in terms of our broadband reach. We are now about number 16 or 20, depending on who you listen to. That is an appalling comment, and one we ought to really take note of as we think about this.

I also support investments in research and development and a bunch of other things that will contribute to the startup of different businesses and firms that are going to unleash our economic potential.

We all in this committee understand the automatic instinct inside a lot of the companies that are interested in this, which says, "Hey, Washington, just leave us alone. We will do fine. We will make this work, and the Internet will grow."

And over the years, I think most of us in this committee have been guided by the belief that in a technology market that is moving so rapidly, that is the right approach in most cases. I have cer-

tainly stood by net neutrality. I have stood by no taxation. I have advocated for as open an architecture as possible in order to unleash the full measure of creative energy and entrepreneurial activity that has really brought this wonder to all of us and continues to innovate.

And I am convinced that we made the right decision in the 1990s here to protect, to do things that did not allow privacy or other issues to somehow eclipse that move for innovation, and I think it might have slowed back then technological advances. But we are in a different place today. We just are in a different place today.

And we need companies like Google and Apple and Facebook to join companies like Intel, eBay, Microsoft, HP, which have already come down on the side of common sense, very restrained, simple privacy protections. We need industry leaders to engage constructively in these legislative efforts to modernize our privacy laws, to come up to the year that we are and the state of art that we are with respect to the marketplace because we want the legislation to work for both the consumer and the entrepreneur.

Now I have reached out to the companies that are here today over the last 6 or 7 months. And I appreciate the time they have taken to work with us so far.

Mr. Chairman, I reject the notion—and one of our colleagues just sort of raised the—you know, we don't—here is what we want to do, but here is what we don't want to do. I reject the notion that privacy protection is the enemy of innovation. It absolutely doesn't have to be and isn't.

In fact, a more trusted information economy, I believe, will encourage greater consumer participation, greater confidence in that marketplace, and, in turn, more and better services in a safer commercial environment that is more respectful of other people. So, in the end, though not in a heavy-handed, overly prescriptive approach, I believe that companies collecting people's information, whether you are a tech titan or not, ought to comply with just a basic code of conduct.

We need to establish what we as a society, in a country that has always valued privacy, what we as a society believes is the sort of basic proper treatment of people's information. I know you can shut off your location services. But that doesn't do the trick because a lot of those services are services we want, and we want to use them.

But we also want to know that what is happening to the information as the consequence of using them is properly protected, that we are properly protected as individuals. I don't think you can continue to create or leave it to firms to decide on an ad hoc basis what that level of protection ought to be.

And I think that is particularly true in an age when the minisupercomputers that are in our pockets are with us almost at all times, and they are almost always on. And particularly among young people, there will be disposition to use most of those apps almost all the time. But it is also true on our computers at home and offline when we buy groceries or when we travel or when we purchase or whatever.

So, as we sit here today, Mr. Chairman, there is no privacy law for general commerce whatsoever. Data collectors alone are setting

the rules. In S. 799, the Commercial Privacy Bill of Rights that Senator McCain and Senator Klobuchar and I have proposed, we propose rules based on fair information practice principles for all collectors of information, including mobile phone and mobile app companies that we will be talking about here today.

And Senator Rockefeller's do-not-track, I think, you know, that is a very important issue, and it is one we ought to be deeply engaged in and, you know, the votes will decide it. But whichever way we go on that, we still need a privacy standard. We still need the basic rules of the road by which everybody agrees we are going to protect commerce, we are going to protect the creative entrepreneurial ability of the Internet, but we are also going to protect individuals or at least give them the knowledge by which they make a decision as to how their information is going to be treated.

I think that those principles include the idea that, regardless of the technology or method used to track Americans, they should know when they are being tracked, why and how long that information is going to be used for, and in what way. And they ought to know with whom that information is going to be shared and be able to reject or accept those practices, and they need legal protections if that respect is not granted to them or the terms of that arrangement are violated.

So I hope, Mr. Chairman, we are going to have a chance at the right moment to tackle this issue within this committee. I think it is a really vital one to Americans growing in its importance.

And I look forward to hearing from the witnesses for the time that I can be here. I apologize I can't be here for the whole time. And I thank you, Mr. Chairman, for your affording us the time to make these statements.

Senator PRYOR. Thank you.

Senator Rockefeller?

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

Senator ROCKEFELLER. Thank you, Mr. Chairman.

I associate myself with every word and comma, perhaps even a semicolon that you have said, Senator Kerry.

I think it is just wrong for people to be wondering about people—you know, we can get into the age business, and I will in a minute. But not knowing what is happening to them, not knowing that they are, in fact, being tracked.

What you said about smartphones are, in fact, supercomputers, little supercomputers. They tell you where you are—tell other people because you make this—and some of you make this information available to other third parties who use it and sell it and make money from it, which is a violation of individual liberties, in my judgment.

Look, we got 234 million mobile devices in use today. Seventy-five percent of teenagers own a cell phone and talk on them and carry them all the time. Seventy-two percent—and this is interesting to me—the wording, even—72 percent of parents say that they have slept with their cell phones.

It is a neutral statement, but it is also——

[Laughter.]

Senator KERRY. In today's world, that is risky.

Senator ROCKEFELLER. Yes. It shows the intensity of this whole thing. You can't—it has got to be under your pillow. I mean, you just can't be without it.

So I think the online privacy issue is not something of an unintended consequence. I think it is a basic American right and a basic American responsibility of the FTC, which I do not think has been very aggressive on this, and of the users, the big companies and all the apps folks. And not just the big ones, but the little ones that just may have three or four people, but there are hundreds of thousands of them that are pumping out apps that are totally unregulated.

And so, the question is what do we do about that? Or what do you do about that? Or do you want us to do something about that? They have to be regulated because they are producing the same things that get people tracked.

I think using a mobile device has an expectation of privacy. And in that, the American people are misled. But I think that is part of the compact that you make when you go into that business.

The companies before us today—Apple, Google, Facebook—I appreciate their being here. They are major players in all of this. And this won't be your last visit, I hope. I hope. In fact, I can assure you, it won't be your last visit.

As the online world grows and evolves, the consumer privacy issues grow and evolve with it. The question is, is anybody watching? Is anybody really paying attention? Are we just saying, "Oh, it is not my responsibility."

If it becomes entirely the responsibility of the Federal Government, people won't like that. So how do you work with consumers so that they can understand the information that is being collected about them? They have that right.

It comes along with the purchase price. That is what they are buying, the right to privacy. They are not getting that, however, and I think that is what we are talking about today.

Smartphones applications allow consumers to access information from all over the world, take and share pictures with friends and family, buy coffee, even videoconferences on the go. Mobile devices are transforming the way consumers access the Internet, record the world around them, and share their lives with others. But with this new innovation comes a gigantic risk.

As smartphones become more powerful, more personal information is being concentrated in one place. These devices are not really phones, as Senator Kerry said. They are miniature computers.

Simple actions now do have unintended consequences. Unintended or intended, I am not sure. But anyway, a lot of people are making a lot of money off the information they collect, without the knowledge of those folks from that.

A mother posting a smartphone picture of her child online may not realize that time and date and location information is also embedded in the picture and available to anyone who can get it, which is pretty much anybody. A teenager accessing an application may not realize that her address book is being assessed and shared with a third party.

That is not meant to happen in this country without the permission of an adult. Four year olds aren't very good at that. Nine year olds aren't very good at that. They don't know how to do that. So maybe we have to do that for them.

And these third parties use this information to target advertising on individuals. It is very cynical. It is very smart. It is very good business, but it is very cynical. It is an abuse of that power, passing on people's profiles.

So everything is new, as John Kerry said. But one thing is clear. Consumers want to understand and have control of their personal information. They have that right. That expectation is not being met. It is not being met.

So I look forward to what our witnesses have to say. Last week, I introduced the Do-Not-Track online bill of 2011. I think that is a terrific bill. It makes it very simple. It just directs the Federal Trade Commission to establish standards by which consumers can tell online companies, including mobile applications, that they do not want their information collected it takes to collect.

Very simple, and it applies to everybody, works on everybody. Then the FTC, of course, would have to make sure that companies respect that choice.

Mr. Chairman, I thank you.

Senator PRYOR. Thank you, Mr. Chairman.

And with the Committee's permission, what I would like to do is go ahead and go to the first panel.

And our first panelist today is David Vladeck. He is Director of the Consumer Protection Bureau of the FTC. We welcome you. We thank you. Glad you are here.

Your statement will be made part of the record, your written statement, as well as everybody else's opening statements, if they would like to submit those, and the next panel's statements as well. So I would ask you to keep your opening remarks to 5 minutes, if possible.

Thank you.

STATEMENT OF DAVID C. VLADECK, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Mr. VLADECK. Chairman Pryor, Chairman Rockefeller, members of the Committee, I am David Vladeck, the Director of the Federal Trade Commission's Bureau of Consumer Protection.

I appreciate the opportunity to present the Commission's testimony on consumer protection issues in the mobile marketplace. The views expressed in the written statement that we submitted represent the Commission's views. My oral remarks and any response to questions represent my own views.

Today's hearing could not be more timely or more important. We are seeing explosive growth in the mobile marketplace. Device technology is constantly improving, robust wireless Internet connections are nearly ubiquitous, businesses are innovating, and consumers are purchasing and using smartphones at extraordinary rates.

And there is no wonder why. Today's smartphones are incredibly powerful, multitasking devices that marry the search capacity of a desktop computer with the personal, always-on, and always-with-

you nature of mobile phones. There is no question that these devices benefit consumers, but there is also no question that these devices raise serious privacy concerns.

These concerns stem from exactly the always-on and always-with-you nature of these devices—the invisible collection and sharing of data with multiple parties; the ability to track consumers, including children and teens, to their precise location; and the difficulty of providing meaningful disclosures and choices about data collection on a smartphone's small screen.

For 40 years, the Federal Trade Commission has worked to protect consumer privacy, and we are working hard to protect consumer privacy in the mobile marketplace. To keep pace with changes in the mobile market, the Commission has hired technologists, created a mobile forensic lab, conducted series of in-house trainings, and assembled a team focused on mobile technology. Every consumer protection investigation now examines the target's use of mobile technology.

Currently, we have a number of nonpublic investigations underway relating to unfair and deceptive practices in the mobile marketplace. The Federal Trade Commission's primary law enforcement tool, the FTC Act, prohibits unfair or deceptive practices, and it applies in all media, including mobile.

Last August, the Commission charged a public relations company with deceptively endorsing mobile gaming apps in the iTunes store. The Commission's recent cases against two of the largest players in the mobile ecosystem, Google and Twitter, further demonstrate the application of the FTC's privacy framework to the mobile marketplace.

As you know, the Commission is currently reviewing whether its privacy framework has kept pace with technological change. Last December, the Commission released a preliminary staff report that proposed a new privacy framework that rests on three recommendations to ease the burden on consumers to protect their own information.

First, privacy by design, baking privacy in at the outset. Second, simpler and streamlined privacy choices. And third, transparency, so consumers know what data is being pulled down and who is getting it and who is using it.

These principles are especially relevant in the mobile marketplace, given all of the concerns related to the invisible collection and sharing of personal information, like the precise geolocation data of children and teens, combined with the difficulty of providing meaningful disclosures in a small-screen environment.

The preliminary report also included a recommendation to implement a universal choice mechanism for behavioral tracking, including behavioral advertising, often referred to as Do-Not-Track. A majority of the Commission has expressed support for such a mechanism. Although the Commission has not taken a position on whether to recommend legislation in this area, the Commission strongly supports the goals of Chairman Rockefeller's Do-Not-Track legislation and supports the approach laid out in that bill, including the scope of the Do-Not-Track standard, the technical feasibility and cost, and how the collection of anonymous data would be treated under the statute.

I also want to commend Senator Kerry and Senator Klobuchar for their work on the Commercial Privacy Bill of Rights, and the members of this committee, including its chair, for their leadership on protecting consumer privacy.

At a time when some children learn how to play games on a smartphone before they learn to tie their shoes, the Commission is also reviewing the Children's Online Privacy Protection Act rule to see whether technological changes in the online environment warrant any changes in the rule and statute.

While the review is still ongoing, remarks at last year's COPPA roundtable, along with public comments we have received, demonstrate widespread consensus that both the COPPA statute and rule were written broadly enough to encompass most forms of mobile communications without the need for statutory change.

In closing, the Commission is committed to protecting consumers in the mobile sphere through law enforcement and by working with industry and consumer groups to develop workable solutions that protect consumers while allowing for innovation.

I am, of course, happy to answer any questions.

[The prepared statement of Mr. Vladeck follows:]

PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION

Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee, I am David C. Vladeck, Director of the Bureau of Consumer Protection of the Federal Trade Commission ("FTC" or "Commission"). I appreciate the opportunity to present the Commission's testimony on consumer protection issues in the mobile marketplace.[1]

This testimony first highlights the expansive growth of the mobile arena and what it means for U.S. consumers. Second, it summarizes the Commission's response to new mobile technologies, the Commission's expansion of its technical expertise, recent law enforcement actions in the mobile arena (adding to the Commission's extensive law enforcement experience in areas relating to the Internet and privacy),[2] and its examination of consumer privacy issues raised by mobile technologies. Third, it discusses the application of a Do Not Track mechanism in the mobile environment.[3] And finally, the testimony discusses the special issues that mobile technologies raise for the privacy of children and teens, and provides an update of the Commission's review of the Children's Online Privacy Protection Rule.

I. The Mobile Marketplace

Mobile technology is exploding with a range of new products and services, and consumers across the country are rapidly responding to the industry's creation of smarter devices. According to the wireless telecommunications trade association, CTIA, the wireless penetration rate reached 96 percent in the United States by the end of last year.[4] Also by that same time, 27 percent of U.S. mobile subscribers owned a smartphone,[5] which is a wireless phone with more powerful computing abilities and connectivity than a simple cell phone. Such mobile devices are essen-

---

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

[2] In the last fifteen years, the FTC has brought more than 30 data security cases; 64 cases against companies for improperly calling consumers on the Do Not Call registry; 86 cases against companies for violating the Fair Credit Reporting Act ("FCRA"); 96 spam cases; 15 spyware cases; and 16 cases against companies for violating the Children's Online Privacy Protection Act.

[3] Commissioner William E. Kovacic dissents from this testimony to the extent that it endorses a Do Not Track mechanism. He believes that the endorsement of a Do Not Track mechanism is premature.

[4] CTIA, *Wireless Quick Facts,* available at *www.ctia.org/advocacy/research/index.cfm/aid/10323*.

[5] ComScore, *The 2010 Mobile Year in Review Report* (Feb. 14. 2011), at 5, available at *www.comscore.com/Press__Events/Presentations__Whitepapers/2011/2010__Mobile__Year__in__Review*.

tially handheld computers that offer Web browsing, e-mail, and a broad range of data services. These new mobile devices allow consumers to handle a multitude of tasks in the palms of their hands and offer Internet access virtually anywhere.

Companies are increasingly using this new mobile medium to provide enhanced benefits to consumers, whether to provide online services or content, or to market other goods or services.[6] For example, consumers can search websites to get detailed information about products, or compare prices on products they are about to purchase while standing in the check-out line. They can join texting programs that provide instantaneous product information and mobile coupons at the point of purchase or download mobile software applications ("apps") that can perform a range of consumer services such as locating the nearest retail stores, managing shopping lists, tracking family budgets, transferring money between accounts, or calculating tips or debts.[7] Apps also allow consumers to read news articles, play interactive games, and connect with family and friends via social networks. Any of these services can contain advertising, including targeted advertising.

II. FTC's Response to Consumer Protection Issues Involving Mobile Technology

New technology can bring tremendous benefits to consumers, but it also can present new concerns and provide a platform for old frauds to resurface. Mobile technology is no different, and the Commission is making a concerted effort to ensure that it has the necessary technical expertise, understanding of the marketplace, and tools needed to monitor, investigate, and prosecute deceptive and unfair practices in the mobile arena.

A. Developing an Understanding of Mobile Issues Through Workshops and Town Halls

For more than a decade, the Commission has explored mobile and wireless issues, starting in 2000 when the agency hosted a two-day workshop studying emerging wireless Internet and data technologies and the privacy, security, and consumer protection issues they raise.[8] In 2006, the Commission held a three-day technology forum that prominently featured mobile issues.[9] Shortly thereafter, the Commission hosted two Town Hall meetings to explore the use of radio frequency identification (RFID) technology, and its integration into mobile devices as a contactless payment system.[10] And in 2008, the Commission held a two-day forum examining consumer protection issues in the mobile sphere, including issues relating to ringtones, games, chat services, mobile coupons, and location-based services.[11] Most recently, as discussed below, the Commission examined the privacy issues raised by mobile technologies as part of a series of roundtables on consumer privacy in late 2009 and early 2010.

B. Developing a Mobile Lab and Creating a Mobile Team

The FTC has hired technologists (including its first Chief Technologist) and invested in new technologies to enable its investigators and attorneys to respond to the growth of mobile commerce and to conduct mobile-related investigations.[12] For

---

[6] Indeed, a recent industry survey found that 62 percent of marketers used some form of mobile marketing for their brands in 2010 and an additional 26 percent reported their intention to begin doing so in 2011. *See* Association of National Advertisers, Press Release, *Vast Majority of Marketers Will Utilize Mobile Marketing and Increase Spending on Mobile Platforms in 2011,* (Jan. 31, 2011) (describing the results of a survey conducted by the Association of National Advertisers and the Mobile Marketing Association), available at *www.ana.net/content/show/id/20953*.

[7] Although Apple's App Store and Google's Android Market are less than 3 years old, they collectively contain more than 600,000 apps. In January 2011, Apple reported that ten billion apps had been downloaded from the App Store. In May 2011, Google announced that 4.5 billion apps had been downloaded from the Android Market. See *www.apple.com/itunes/10-billion-app-countdown/; googleblog.blogspot.com/2011/05/android-momentum-mobile-and-more-at.html*.

[8] FTC Workshop, *The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues,* available at *www.ftc.gov/bcp/workshops/wireless/index.shtml*.

[9] FTC Workshop, *Protecting Consumers in the Next Tech-ade,* available at *www.ftc.gov/bcp/workshops/techade.* The Staff Report is available at *www.ftc.gov/os/2008/03/P064101tech.pdf*.

[10] FTC Workshop, *Pay on the Go: Consumers and Contactless Payment,* available at *www.ftc.gov/bcp/workshops/payonthego/index.shtml;* FTC Workshop, *Transatlantic RFID Workshop on Consumer Privacy and Data Security,* available at *www.ftc.gov/bcp/workshops/transatlantic/index.shtml*.

[11] FTC Workshop, *Beyond Voice: Mapping the Mobile Marketplace,* available at *www.ftc.gov/bcp/workshops/mobilemarket/index.shtml*.

[12] *See, e.g.,* Press Release, *FTC Adds Edward W. Felten as its Chief Technologist* (Nov. 4, 2010), available at *www.ftc.gov/opa/2010/11/cted.shtm*.

many years, FTC Bureau of Consumer Protection staff have investigated online fraud using the agency's Internet Lab, a facility that contains computers with IP addresses not assigned to the government, as well as evidence-capturing software. The agency has expanded the Internet lab to include mobile devices spanning various platforms and carriers, along with the software and other equipment needed to collect and preserve evidence.

Additionally, the FTC's Bureau of Consumer Protection assembled a team focusing on mobile technology. This group is conducting research, monitoring the various platforms, app stores, and applications, and training other FTC staff on mobile issues. In addition, in all of the FTC's consumer protection investigations, staff is examining whether the targets of investigations are using mobile technology in their operations.

C. Applying the FTC Act to the Mobile Arena

Although the FTC does not enforce any special laws applicable to mobile marketing, the FTC's core consumer protection law—Section 5 of the FTC Act—prohibits unfair or deceptive practices in the mobile arena.[13] This law applies to commerce in all media, whether traditional print, telephone, television, desktop computer, or mobile device. The Commission has several recent law enforcement and policy initiatives in the mobile arena, which build on the Commission's extensive law enforcement experience in the Internet and privacy areas.

1. Endorsement Law and Advertising Substantiation

The FTC brought a case last August applying FTC advertising law principles to the mobile apps marketplace. The Commission charged Reverb Communications, Inc., a public relations agency hired to promote video games, with deceptively endorsing mobile gaming applications in the iTunes store.[14] The company allegedly posted positive reviews of gaming apps using account names that gave the impression the reviews had been submitted by disinterested consumers when they were, in actuality, posted by Reverb employees. In addition, the Commission charged that Reverb failed to disclose that it often received a percentage of the sales of each game. The Commission charged that the disguised reviews were deceptive under Section 5, because knowing the connections between the reviewers and the game developers would have been material to consumers reviewing the iTunes posts in deciding whether or not to purchase the games. In settling the allegations, the company agreed to an order prohibiting it from publishing reviews of any products or services unless it discloses a material connection, when one exists, between the company and the product.

The *Reverb* settlement demonstrates that the FTC's well-settled truth-in-advertising principles apply to new forms of mobile marketing. The mobile marketplace may offer advertisers new opportunities, but as in the offline world, companies must be able to substantiate claims made about their products. Developers may not make misrepresentations or unsubstantiated claims about their mobile apps, whether those claims are in banner ads, on a mobile website, in an app, or in app store descriptions. FTC staff is working to identify other violations of these well-established principles in the mobile context.

2. Unauthorized Charges and Other Deceptive Conduct

FTC staff has active investigations into other unfair or deceptive conduct in the mobile arena. For example, staff is examining both the cramming of charges on consumers wireless phone bills and alleged inadequate disclosures of charges for in-app purchases.

Cramming is the practice of placing unauthorized charges on consumers' telephone bills. The FTC has aggressively prosecuted cramming violations in connection with landline telephone bills for many years.[15] Mobile telephone accounts can also be used as a billing mechanism. On May 11, the FTC hosted a workshop on Phone Bill Cramming. The workshop examined how the mobile and landline billing platforms work, best practices for industry, and the development of cramming prevention mechanisms.[16]

---

[13] 15 U.S.C. § 45(a).

[14] *Reverb Commc'ns, Inc.,* FTC Docket No. C–4310 (Nov. 22, 2010) (consent order), available at *www.ftc.gov/opa/2010/08/reverb.shtm*.

[15] *See, e.g., FTC* v. *INC21.com,* No. C 10–00022 WHA (N.D. Cal.) (summary judgment entered Sept. 21, 2010), available at *www.ftc.gov/opa/2010/09/inc21.shtm; FTC* v. *Nationwide Connections, Inc.,* No. Cv 06–80180 (S.D. Fla.) (final stipulated orders entered Apr. 11, 2008), available at *www.ftc.gov/opa/2008/04/cram.shtm*.

[16] *See* FTC Workshop, *Phone Bill Cramming,* available at *www.ftc.gov/bcp/workshops/cramming/*.

Concerns about charges for in-app purchases in games and other apps that initially appear to be free is another issue of concern. Several Members of Congress and others have raised concerns about purportedly free mobile apps directed to children that subsequently result in charges for products and services found within the applications, without adequate disclosures.[17] FTC staff is examining industry practices related to this issue.

3. Unsolicited Commercial Text Messages

Through enforcement of the CAN–SPAM Act,[18] the Commission has long sought to protect consumers from unsolicited commercial e-mail. Indeed, CAN-SPAM applies to e-mail regardless of what type of computer or device is used to view and send the commercial e-mail messages. Unsolicited text messages present problems similar to those addressed by CAN–SPAM, but unsolicited text messages present additional problems for mobile phone users.

In February, the Commission filed its first law enforcement action against a sender of unsolicited text messages and obtained a temporary restraining order suspending the defendant's challenged operations. The FTC alleged that Philip Flora sent more than 5 million unsolicited text messages—almost a million a week—to the mobile phones of U.S. consumers and that this was an unfair practice under Section 5 of the FTC Act.[19] Many consumers who received Flora's text messages—which typically advertised questionable mortgage loan modification or debt relief services—had to pay a fee each time they received a message. Many others found that Flora's text messages caused them to exceed the number of messages included in their mobile service plans, thereby causing some consumers to incur additional charges on their monthly bill.[20]

4. Debt Collection Technology

The impact of mobile technology is also evident in the debt collection industry. On April 28, the Commission hosted a forum that examined the impact of new technologies on debt collection practices, including the technologies used to locate, identify, and contact debtors.[21] Panelists discussed the consumer concerns that arise when collectors contact debtors on their mobile phones, and whether some appropriate consumer consent should be required before a collector calls or sends text messages to a consumer's mobile phone. Commission staff is considering and analyzing the information received from the workshop and is preparing a summary report.

5. Mobile Payments

The use of mobile phones as a payment device also presents potential consumer protection issues.[22] As mentioned above, consumers can already charge goods and services, real or virtual, to their mobile telephone bills and app store accounts. Many other payment mechanisms and models are still developing, such as contactless payments systems that allow consumers to pay for products and services with the swipe of their smart phone.[23] Many, but not all, mobile payment systems

---

[17] Cecelia Kang, *Lawmakers Urge FTC to Investigate Free Kids Games on iPhone, Washington Post* (Feb. 8, 2011), available at *www.washingtonpost.com/wp-dyn/content/article/2011/02/08/AR2011020805721.html*.

[18] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C. §§ 7701–7713.

[19] *FTC* v. *Flora,* CV11–00299 (C.D. Cal.) (Compl. filed Feb. 22, 2011), available at *www.ftc.gov/opa/2011/02/loan.shtm*. The complaint also alleges that Flora sent over the Internet unsolicited commercial e-mail messages advertising his texting services. The e-mails did not include a valid opt-out mechanism and failed to include a physical postal address, in violation of the CAN–SPAM Act. In these e-mails, Flora offered to send 100,000 text messages for only $300. Further, the complaint charged that Flora deceptively claimed an affiliation with the Federal Government in connection with the loan modification service advertised in the text messages.

[20] While the financial injury suffered by any consumer may have been small, the aggregate injury was likely quite large. And, even for those consumers with unlimited messaging plans, Flora's unsolicited messages were harassing and annoying, coming at all hours of the day.

[21] FTC Workshop, *Debt Collection 2.0: Protecting Consumers as Technologies Change,* available at *www.ftc.gov/bcp/workshops/debtcollectiontech/index.shtml*.

[22] *See* Elizabeth Eraker, Colin Hector & Chris Hoofnagle, *Mobile Payment: The Challenge of Protecting Consumers and Innovation,* BNA, 10 Privacy & Security Law Report 212 (Feb. 7, 2011).

[23] *See* Darin Contini, Marianne Crowe, Cynthia Merritt, Richard Oliver & Steve Mott, Retail Payments Risk Forum, *Mobile Payments in the United States: Mapping Out the Road Ahead,* (Mar. 25, 2011), available at *www.frbatlanta.org/documents/rprf/rprf_pubs/110325_wp.pdf;* Smart Card Alliance, *Contactless Payment Growth and Evolution to Mobile NFC Payment are*

Continued

are tied to traditional payment mechanisms such as credit cards. Staff is monitoring this emerging area for potential unfair or deceptive practices.

III. Privacy Issues in the Mobile Arena

The rapid growth of new mobile services has provided enormous benefits to both businesses and consumers. At the same time, it has facilitated unprecedented levels of data collection, which are often invisible to consumers.

The Commission recognizes that mobile technology presents unique and heightened privacy and security concerns. In the complicated mobile ecosystem, a single mobile device can facilitate data collection and sharing among any entities, including wireless providers, mobile operating system providers, handset manufacturers, app developers, analytics companies, and advertisers. And, unlike other types of technology, mobile devices are typically personal to the user, almost always carried by the user and switched-on.[24] From capturing consumers' precise location to their interactions with e-mail, social networks, and apps, companies can use a mobile device to collect data over time and "reveal[ ] the habits and patterns that mark the distinction between a day in the life and a way of life."[25] Further, the rush of on-the-go use, coupled with the small screens of most mobile devices, makes it especially unlikely that consumers will read detailed privacy disclosures.

In recent months, news reports have highlighted the virtually ubiquitous data collection by smartphones and their apps. Researchers have reported that both major smartphone platform providers collect precise location information from phones running their operating systems to support their device location services.[26] The *Wall Street Journal* has documented numerous companies gaining access to detailed information—such as age, gender, precise location, and the unique identifiers associated with a particular mobile device—that can be used to track and predict consumers' every move.[27] Not surprising, recent surveys indicate that consumers are concerned. For example, a recent Nielsen study found that a majority of smartphone app users worry about their privacy when it comes to sharing their location through a mobile device.[28] The Commission has addressed these issues through a combination of law enforcement and policy initiatives, as discussed below.

A. Mobile Privacy: Enforcement Actions

The FTC's privacy cases have challenged companies that fail to protect the privacy and security of consumer information, including information obtained through mobile communications. Two recent cases highlight the application of the FTC's privacy enforcement to the mobile marketplace.

First, the Commission's recent case against Google alleges that the company deceived consumers by using information collected from Gmail users to generate and populate a new social network, Google Buzz.[29] The Commission charged that Gmail users' associations with their frequent e-mail contacts became public without the users' consent. As part of the Commission's proposed settlement order, Google must

---

Highlights as Smart Card Alliance/CTST Conference Opens (May 14, 2008), available at *www.smartcardalliance.org/articles/2008/05/14/contactless-payment-growth-and-evolution-to-mobile-nfc-payment-are-highlights-as-smart-card-alliance-ctst-conference-opens*.

[24] *See, e.g.,* Amanda Lenhart, Pew Internet & American Life Project, *Adults, Cell Phones and Texting* (Sept. 2, 2010), at 10, available at *www.pewinternet.org/Reports/2010/Cell-Phones-and-American-Adults/Overview.aspx* ("65 percent of adults with cell phones say they have ever slept with their cell phone on or right next to their bed"); Amanda Lenhart, Rich Ling, Scott Campbell, Kristen Purcell, Pew Internet & American Life Project, *Teens and Mobile Phones* (Apr. 20, 2010), at 73, available at *www.pewinternet.org/Reports/2010/Teens-and-Mobile-Phones/Chapter-3/Sleeping-with-the-phone-on-or-near-the-bed.aspx* (86 percent of cell-owning teens ages 14 and older have slept with their phones next to them).

[25] *United States* v. *Maynard,* 615 F.3d 544, 562 (D.C. Cir. 2010).

[26] *See* Julia Angwin & Jennifer Valentino-Devries, *Apple, Google Collect User Data,* Wall St. J. (Apr. 22, 2011), available at *online.wsj.com/article/SB10001424052748703983704576277101723453610.html*

[27] *See, e.g.,* Robert Lee Hotz, *The Really Smart Phone,* Wall St. J. (Apr. 23, 2011), available at *online.wsj.com/article/SB10001424052748704547604576263__261679848814.html* (describing how researchers are using mobile data to predict consumers' actions); Scott Thurm & Yukari Iwatane Kane, *Your Apps are Watching You,* Wall St. J. (Dec. 18, 2010), available at *online.wsj.com/article/SB10001424052748704368004576027751867039730.html* (documenting the data collection that occurs through many popular smartphone apps).

[28] NielsenWire, *Privacy Please! U.S. Smartphone App Users Concerned with Privacy When it Comes to Location* (Apr. 21, 2011), available at *blog.nielsen.com/nielsenwire/online_mobile/privacy-please-u-s-smartphone-app-users-concerned-with-privacy-when-it-comes-to-location; see also* Ponemon Institute, *Smartphone Security: Survey of U.S. Consumers* (Mar. 2011), at 7, available at *aa-download.avg.com/filedir/other/__Smartphone.pdf* (64 percent of consumers worry about being tracked when using their smartphones).

[29] *Google, Inc.,* FTC File No. 102 3136 (Mar. 30, 2011) (consent order accepted for public comment), available at *www.ftc.gov/opa/2011/03/google.shtm*.

protect the privacy of all of its customers—including mobile users. For example, the order requires Google to implement a comprehensive privacy program and conduct independent audits every other year for the next 20 years.

Second, in the Commission's case against social networking service Twitter, the FTC alleged that serious lapses in the company's data security allowed hackers to obtain unauthorized administrative control of Twitter.[30] As a result, hackers had access to private "tweets" and non-public user information—including users' mobile phone numbers—and took over user accounts, among them, those of then-President-elect Obama and Rupert Murdoch. The Commission's order, which applies to Twitter's collection and use of consumer data, including through mobile devices or apps, prohibits future misrepresentations and requires Twitter to maintain reasonable security and obtain independent audits of its security practices.

FTC staff has a number of additional active investigations regarding privacy issues associated with mobile devices, including children's privacy.

B. Mobile Privacy: Policy Initiatives

In late 2009 and early 2010, the Commission held three roundtables to examine how changes in the marketplace have affected consumer privacy and whether current privacy laws and frameworks have kept pace with these changes.[31] At one roundtable, a panel focused on the privacy implications of mobile technology. Participants addressed the complexity of data collection through mobile devices; the extent and nature of the data collection, particularly with respect to location data; and the adequacy of privacy disclosures on mobile devices.[32] Based on the information received through the roundtables, FTC staff drafted a preliminary report ("Staff Report") proposing a new privacy framework consisting of three main recommendations, each of which applies to mobile technology.[33]

First, FTC staff recommended that companies adopt a "privacy by design" approach by building privacy protections into their everyday business practices, such as not collecting or retaining more data than they need to provide a requested service or transaction. Thus, for example, if an app provides only traffic and weather information to a consumer, it does not need to collect call logs or contact lists from the consumer's device.

Second, staff recommended that companies provide simpler and more streamlined privacy choices to consumers. This means that all companies involved in data collection and sharing through mobile devices—carriers, handset manufacturers, operating system providers, app developers, and advertisers—should work together to provide such choices and to ensure that they are understandable and accessible on the small screen. The Staff Report also stated that companies should obtain affirmative express consent before collecting or sharing sensitive information, such as precise location data.

Third, the Staff Report proposed a number of measures that companies should take to make their data practices more transparent to consumers, including streamlining their privacy disclosures to consumers.

After releasing the Staff Report, staff received 452 public comments on its proposed framework, a number of which implicate mobile privacy issues specifically. FTC staff is analyzing the comments and will take them into consideration in preparing a final report for release later this year.

C. Web Browsing and Do Not Track on Mobile Devices

The Staff Report included a recommendation to implement a universal choice mechanism for online tracking, including for purposes of delivering behavioral advertising, often referred to as "Do Not Track," and a majority of the Commission has expressed support for such a mechanism.[34] Behavioral advertising helps support

---

[30] *Twitter, Inc.,* FTC Docket No. C–4316 (Mar. 2, 2011) (consent order), available at *www.ftc.gov/opa/2011/03/twitter.shtm*.

[31] *See* FTC, *Exploring Privacy: A Roundtable Series,* available at *http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml*.

[32] Transcript of Roundtable Record, *Exploring Privacy: A Roundtable Series* (Jan. 28, 2010) (Panel 4, "Privacy Implication of Mobile Computing"), at 238, available at *http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Jan2010_Transcript.pdf*.

[33] *See* FTC Preliminary Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010), available at *http://ftc.gov/os/2010/12/101201privacyreport.pdf*. Commissioners William E. Kovacic and J. Thomas Rosch issued concurring statements available at *http://ftc.gov/os/2010/12/101201privacyreport.pdf* at Appendix D and Appendix E, respectively.

[34] *See* FTC Staff Report, *supra* note 33; *see also Do Not Track: Hearing Before the Subcomm. on Commerce, Trade and Consumer Prot. of the H. Comm. on Energy and Commerce*, 111th Cong. (Dec. 2, 2010), available at *www.ftc.gov/os/testimony/101202donottrack.pdf* (statement of

Continued

online content and services, and many consumers may value the personalization that it offers. However, the third-party tracking that underlies much of this advertising is largely invisible to consumers, some of whom may prefer not to have their personal browsing and searching information collected by companies with which they do not have a relationship.

The FTC repeatedly has called on stakeholders to develop and implement better tools to allow consumers to control the collection and use of their online browsing data,[35] and industry and other stakeholders have responded. In recent months a number of browser vendors—including Microsoft, Mozilla, and Apple—have announced that the latest versions of their browsers include, or will include, the ability for consumers to tell websites not to track their online activities.[36] Additionally, last month the World Wide Web Consortium [37] held a two-day workshop at which participants including academics, industry representatives, and privacy advocates discussed how to develop standards for incorporating "Do Not Track" preferences into Internet browsing.[38] The online advertising industry has also made important progress in this area. For example, the Digital Advertising Alliance, an industry coalition of media and marketing associations, is launching an enhanced notice program that includes an icon embedded in behaviorally targeted ads.[39] When consumers click on the icon, they can see more information about how the ad was targeted and delivered to them and are given the opportunity to opt out of receiving such ads, although collection of browsing information could continue.

These recent industry efforts to improve consumer control are promising, but they are still in the early stage and their effectiveness remains to be seen. As industry continues to explore technical options and implement self-regulatory programs and Congress continues to examine Do Not Track, five critical principles should be considered to make any Do Not Track mechanism robust and effective. Do Not Track should (1) be universal; (2) be easy to find and use; (3) be enforceable; (4) ensure that consumer choices are persistent; and (5) not only allow consumers to opt out of receiving targeted advertising, but also allow them to opt out of collection of behavioral data for all purposes that are not commonly accepted.[40]

The Staff Report asked whether Do Not Track should apply in the mobile context. At least for purposes of Web browsing, the issues surrounding implementation of Do

---

the FTC, Commissioner Kovacic dissenting). Commissioner Kovacic believes that the endorsement of a Do Not Track mechanism by staff (in the report) and the Commission (in this testimony) is premature. *See* FTC Staff Report, App. D. Commissioner Rosch supported a Do Not Track mechanism only if it were "technically feasible" and implemented in a fashion that provides informed consumer choice regarding all the attributes of such a mechanism. *See id.*, App. E. To clarify, Commissioner Rosch continues to believe that a variety of questions need to be answered prior to the endorsement of any particular Do Not Track mechanism, including the consequences of the mechanism for consumers and competition.

[35] *See, e.g., The State of Online Consumer Privacy, Hearing Before the S. Comm. on Commerce, Science & Transportation,* 112th Cong. (Mar. 16, 2011), available at *www.ftc.gov/os/testimony/110316consumerprivacysenate.pdf* (statement of the FTC, Commissioner Kovacic dissenting); *Do Not Track: Hearing Before the Subcomm. on Commerce, Trade and Consumer Prot. of the H. Comm. on Energy and Commerce,* 111th Cong. (Dec. 2, 2010), available at *www.ftc.gov/os/testimony/101202donottrack.pdf* (statement of the FTC, Commissioner Kovacic dissenting); *see also FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* (Feb. 2009), available at *www.ftc.gov/os/2009/02/P085400behavadreport.pdf.*

[36] *See* Press Release, *Microsoft, Providing Windows Customers with More Choice and Control of Their Privacy Online with Internet Explorer 9* (Dec. 7, 2010), available at *www.microsoft.com/presspass/features/2010/dec10/12–07ie9privacyqa.mspx;* Mozilla Blog, *Mozilla Firefox 4 Beta, Now Including "Do Not Track" Capabilities, blog.mozilla.com/blog/2011/02/08/mozilla-firefox–4-beta-now-including-do-not-track-capabilities/* (Feb. 8, 2011); Nick Wingfield, *Apple Adds Do-Not-Track Tool to New Browser,* Wall St. J. (Apr. 14, 2011), available at *online.wsj.com/article/SB10001424052748703551304576261272308358858.html.*

[37] The World Wide Web Consortium (W3C) is an international community whose "mission is to lead the World Wide Web to its full potential by developing protocols and guidelines that ensure the long-term growth of the Web." *See www.w3.org/Consortium/mission.html.*

[38] *See www.w3.org/2011/track-privacy/.* This event followed a joint proposal by Stanford Law School's Center for Internet and Society and Mozilla for a header-based Do Not Track mechanism submitted to the Internet Engineering Task Force. *See* Do Not Track: A Universal Third-Party Web Tracking Opt Out (Mar. 7, 2011), available at *tools.ietf.org/html/draft-mayer-do-not-track-00; see also Mozilla Makes Joint Submission to IETF on DNT,* available at *firstperson cookie.wordpress.com/2011/03/09/mozilla-makes-joint-submission-to-ietf-on-dnt/.*

[39] *See* Interactive Advertising Bureau Press Release, *Major Marketing Media Trade Groups Launch Program to Give Consumers Enhanced Control over Collection and Use of Web Viewing Data for Online Behavioral Advertising* (Oct. 4, 2010), available at *www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr–100410.*

[40] For more detail concerning these five principles, *see The State of Online Consumer Privacy, Hearing Before the S. Comm. on Commerce, Science & Transportation, supra* note 35, at 16–17.

Not Track are the same on mobile devices and desktop computers. On both types of devices, the user could assert a Do Not Track choice, the browser would remember this choice, and the browser would send the Do Not Track request to other websites visited. The technology underlying mobile apps, however, differs in some respects from Web browsing (apps run outside of the browser, unlike websites), and thus the Staff Report has asked for comment about the application of Do Not Track to mobile apps, and FTC staff is currently examining the technology involved in a Do Not Track mechanism for mobile apps.

Chairman Rockefeller has introduced Do Not Track legislation that would address desktop and mobile services.[41] The Commission supports the fundamental goals of this legislation—to provide transparency and consumer choice regarding tracking. Although the Commission has not taken a position on whether there should be legislation in this area, the Commission supports the approach in the proposed legislation, which would consider a variety of factors in implementing a Do Not Track mechanism, including the scope of the Do Not Track standard, the technical feasibility and costs, and how the collection of anonymous data would be treated under the standard. Indeed, the Commission agrees that any legislative mandate must give careful consideration to these issues, along with any competitive implications, as part of the Do Not Track rulemaking process. We would be pleased to work with Chairman Rockefeller, the Committee and Committee staff as they consider these important issues.

D. Children's and Teens' Mobile Privacy

The Commission has a long history of working to protect the privacy of young people in the online environment. In recent years, the advent of new technologies and new ways to collect data, including through mobile devices, has heightened concerns about the protection of young people when online.

1. Children's and Teen's Use of Mobile Technology

Children's and teens' use of mobile devices is increasing rapidly—in 2004, 45 percent of 12 to 17 year-olds had a cell phone; by 2009, that figure jumped to 75 percent.[42] Many young people are using their phones not just for calling or sending text messages, but increasingly for sending e-mails, Web browsing, and using a host of apps that enable them to access social networks and make online purchases.[43] They are also using relatively new mobile apps that raise privacy concerns such as location-based tracking.[44] Even very young children have embraced these new technologies. In one study, two-thirds of the children ages 4–7 stated they had used an iPhone, often one owned by a family member and handed back to them while riding in an automobile.[45]

2. Enforcement of the Children's Online Privacy Protection Rule

The Commission actively engages in law enforcement, consumer and business education, and rulemaking initiatives to ensure knowledge of, and adherence to, the Children's Online Privacy Protection Rule ("COPPA Rule"), issued pursuant to the Children's Online Privacy Protection Act of 1998.[46] The COPPA Rule requires operators of interactive websites and online services directed to children under the age of 13, as well as operators of general audience sites and services having knowledge that they have collected information from children, to provide certain protections. In the past 10 years, the Commission has brought 16 law enforcement actions alleging COPPA violations and has collected more than $6.2 million in civil penalties.

Just last week, the Commission announced its largest civil penalty in a COPPA action, a $3 million settlement against Playdom, Inc. The Commission alleged that the company, a leading developer of online multi-player games, as well as one of its executives, violated COPPA by illegally collecting and disclosing personal information from hundreds of thousands of children under age 13 without their parents'

---

[41] Do Not Track Online Act of 2011, S. 913, 112th Cong. (2011)

[42] Amanda Lenhart, Rich Ling, Scott Campbell, Kristen Purcell, Pew Internet & American Life Project, *Teens and Mobile Phones* (Apr. 20, 2010), at 2, available at *www.pewinternet.org/~/media//Files/Reports/2010/PIP-Teens-and-Mobile–2010.pdf*.

[43] *Id.*

[44] Nielsen, *How Teens Use Media* (June 2009), available at *blog.nielsen.com/nielsenwire/reports/nielsen_howteensusemedia_june09.pdf*.

[45] Cynthia Chiong & Carly Shuler, Joan Ganz Cooney Center, *Learning: Is there an App for that?* (Nov. 2010), at 15, available at *www.joanganzcooneycenter.org/upload_kits/learning apps_final_110410.pdf*.

[46] The Commission's COPPA Rule is found at 16 C.F.R. Part 312. The COPPA statute is found at 15 U.S.C. § 6501 *et seq*.

prior consent.[47] While the allegations against Playdom do not specifically include the collection of information via mobile communications, the order, like all previous COPPA orders, applies to future information collected from children, whether it is collected via a desktop computer or a mobile computing device.

3. Review of the COPPA Rule

In April 2010, the Commission accelerated its review of the COPPA Rule, asking for comment on whether technological changes in the online environment warrant any changes to the Rule or to the statute.[48] In June 2010, the Commission also held a public roundtable to discuss the implications for COPPA enforcement raised by new technologies, including the rapid expansion of mobile communications.[49]

While the Rule review is ongoing, public comments and roundtable remarks reveal widespread consensus that the COPPA statute and the Rule were written broadly enough to encompass most forms of mobile communications without the need for statutory change.[50] For example, current technologies such as mobile applications, interactive games, voice-over-Internet services, and social networking services that access the Internet or a wide-area network are "online services" covered by COPPA.[51] There was less consensus as to whether certain mobile communications such as text messages are "online services" covered by COPPA. Certain commenters indicated that, depending on the details of the texting program—and provided that personal information is collected—COPPA could cover such programs.[52] Other commenters maintained that text messages cross wireless service providers' networks and short message service centers, not the public Internet, and that therefore such services are not Internet-based and are not "online services.[53] Commission staff is assessing new technologies to determine whether they are encompassed by, and conducted in accordance with, COPPA's parameters.

4. Consumer Education Initiatives for Children and Teens

The FTC has launched a number of education initiatives designed to encourage consumers of all ages to use technology safely and responsibly. In particular, the Commission's educational booklet, *Net Cetera: Chatting with Kids About Being Online,*[54] provides practical tips on how parents, teachers, and other trusted adults can help children of all ages, including teens and pre-teens, reduce the risks of inappropriate conduct, contact, and content that come with living life online. *Net Cetera* focuses on the importance of communicating with children about issues ranging from cyber bullying to sexting, social networking, mobile phone use, and online privacy. The Commission has partnered with schools, community groups, and local law enforcement to publicize *Net Cetera,* and the agency has distributed more than 7.8 mil-

---

[47] *United States* v. *Playdom, Inc.,* No. SACV11–00724 (C.D. Cal.) (final stipulated order filed May 11, 2011), available at *www.ftc.gov/opa/2011/05/playdom.shtm*.

[48] *See* 75 Fed. Reg. 17,089 (Apr. 5, 2010). Although, of course, the Commission does not have the authority to amend the statute, it could recommend changes to Congress if warranted. Commission staff anticipates that proposed changes to the COPPA Rule, if any, will be announced in the next few months.

[49] Information about the June 2, 2010 COPPA Roundtable is located at *http://www.ftc.gov/bcp/workshops/coppa/index.shtml*. The public comments submitted in connection with the COPPA Rule review are available at *http://www.ftc.gov/os/comments/copparulerev2010/index.shtm*.

[50] *See, e.g.,* Comment of Center for Democracy and Technology (July 1, 2010), at 2, available at *http://www.ftc.gov/os/comments/copparulerev2010/547597–00049–54858.pdf*; Transcript of Roundtable Record, *COPPA Rule Review Roundtables* (June 2, 2010), at 14, (remarks of Ed Felten, Center for Information Technology Policy), available at *http://www.ftc.gov/bcp/workshops/coppa/__COPPARuleReview__Transcript.pdf* (hereinafter "COPPA Transcript").

[51] The statute's definition of "Internet," covering the "myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol," is plainly device neutral. 15 U.S.C. § 6502(6). In addition, the statutory use of the terms "website located on the Internet" and "online service," although undefined, is broadly understood to cover content that users can access through a browser on an ordinary computer or a mobile device, and services available over the Internet or that connect to the Internet or a wide-area network. *See* Comment of AT&T, Inc. (July 12, 2010), at 5, available at *www.ftc.gov/os/comments/copparulerev2010/547597–00074–54989.pdf*; Comment of Spratt (Apr. 18, 2010), available at *www.ftc.gov/os/comments/copparulerev2010/__547597-00004.html*; COPPA Transcript, *supra* note 50, at 15 (remarks of Ed Felten).

[52] *See* COPPA Transcript, *supra* note 50, at 27–28 (remarks of Ed Felten).

[53] *See* Comment of CTIA (June 30, 2010), at 2–5, available at *www.ftc.gov/os/comments/copparulerev2010/547597–00039–54849.pdf* (citing the Federal Communications Commission's rules and regulations implementing the CAN–SPAM Act of 2003 and the Telephone Consumer Protection Act of 1991, finding that phone-to-phone SMS is not captured by Section 14 of CAN–SPAM because such messages do not have references to Internet domains).

[54] *Net Cetera* is available online at *www.onguardonline.gov/pdf/tec04.pdf*.

lion print copies of the guide since it was introduced in October 2009. FTC staff are currently developing additional consumer education materials focused on mobile issues.

IV. Conclusion

The Commission is committed to protecting consumers, including children and teens, from unfair and deceptive acts in the burgeoning mobile marketplace. This dedication is reflected in the Commission's recent law enforcement actions and ongoing investigations, policy initiatives, and investment of resources to augment its mobile technical expertise and investigative tools. Protecting the privacy and security of consumer information is a critical component of the Commission's focus on mobile technologies and services. We will continue to bring law enforcement actions where appropriate and work with industry and consumer groups to develop workable solutions that allow companies to continue to innovate and give consumers the new products and services they desire.

Senator PRYOR. Thank you very much.

And because we have a full committee here, almost a full subcommittee, I am going to just ask a couple of questions, then I will turn it over to my colleagues.

Thank you very much, Mr. Vladeck, for being here. You mentioned that this is a small-screen world. And even when you have a large screen and you get all these privacy notices and agreements that are online, et cetera, there is a lot of verbiage there you have to go through. So it seems to me that we have a particular challenge in the small-screen world to have meaningful disclosure.

Have you given that much thought, and do you have a solution on that?

Mr. VLADECK. Well, we have addressed this issue in our privacy report, and one of the reasons why we did this privacy rethink at the outset was because even on big screens, privacy policies are often indecipherable to consumers. And simply translating that to the smartphone world, where a consumer might have to click through a dozen, two or three dozen screens to read a privacy policy, doesn't make sense.

We have called for simple, clear, and concise disclosures that can tell consumers—that tell consumers the fundamental information they need to know—what data is being taken, for what purpose, and by whom. Those are the three essential questions, and we think—I am sorry?

Senator PRYOR. So bottom-line disclosure is what you mean?

Mr. VLADECK. Bottom-line disclosure just in time.

Senator PRYOR. Mm-hmm. OK. And let me ask about the geo-tracking capability? Is there a purpose for that? I mean, is there a legitimate business reason why geo-tracking would be available in some apps?

Mr. VLADECK. Well, in some apps, if you are using a map function, geolocation tracking will enhance functionality. That doesn't explain why other apps that do not need geolocation data for functionality are, nonetheless, pulling down geolocation data.

And that is part of the problem. You are given a prompt on some phones, do you want to share your geolocation data? If you say no, you can't use the app.

And that gets back to Senator Kerry's point. You want functionality, but you also want to know who else may be getting access to that data. Is that access just being used to enhance the functionality, or is it then being sent to analytics companies and

ad networks and advertisers and so forth? That information is currently not available to consumers.

Senator PRYOR. And my experience has been when I talk to people about this, they have no clue that this data is being transmitted or shared with anyone. They have no idea. Do you have any statistics on what people know now? I mean, is there any way to know exactly what people understand about this data right now?

Mr. VLADECK. There have been surveys, and the surveys confirm your impression, which is most people don't know. And there is a reason for that. People are not told with whom the data is going to be shared. And so, it is hard to point the finger at the consumer. The consumer just has no way of knowing that on most apps.

Senator PRYOR. Thank you.

Now the order that I was going to call on folks, Chairman Rockefeller, and then we will do the early bird rule. Senator Kerry—no, you are not at the end. You should be at the end, but you are not at the end. Senator Kerry, Senator Klobuchar, and I know Senator Heller just stepped out, and Senator Blunt.

So, Mr. Chairman?

Senator ROCKEFELLER. OK. Since 2000, COPPA has been in effect. It prohibits companies from targeting children 12 years old or younger. It is widely disregarded. Do you agree?

Mr. VLADECK. I don't know whether I would agree with that. We do fairly aggressive enforcement under COPPA. Last week, we announced a settlement against Playdom, one of the largest children's gaming companies, for a civil penalty of $3 million, the largest civil penalty by three times——

Senator ROCKEFELLER. Well, they were disregarding it at least?

Mr. VLADECK. They were disregarding it, and the order applies not simply to the Internet, but for T-Mobile——

Senator ROCKEFELLER. The idea would be that this would not be available without parents' consent. Is that correct?

Mr. VLADECK. It shouldn't have been available. That is correct. The violation there was not—was retaining information without parental consent.

Senator ROCKEFELLER. OK. So if you get a lot of software applications available for popular mobile devices, such as iPhone or Android phone, they qualify, in my mind, as an online service. I am not sure they qualify in their mind as an online service. Could you talk about that?

Mr. VLADECK. Well, we held a workshop in June of last year to discuss exactly these issues. And I think there was widespread consensus that, for example, to use your illustration, that mobile apps would be an online service and, therefore, would be covered by COPPA. And we have reinforced that with our order in Playdom, which makes it quite clear that mobile delivery of these apps is covered by our order and is subject to COPPA.

Senator ROCKEFELLER. And that act requires—you have to provide conspicuous notice on what personal information is being collected and how it is being used.

Mr. VLADECK. That is what the statute says.

Senator ROCKEFELLER. That is under the law—receive parental consent and provide parents with access to all information being collected about their kids.

Now, any of these provisions, a violation of any of them, constitutes a very bad thing under the Federal Trade Commission's act. So the question is such violations are subject to civil penalties. How much do you go after these folks?

Mr. VLADECK. Well, as I said, we have done quite a number of COPPA cases lately, and we have a number of investigations ongoing into the mobile space, including apps directed at children.

Senator ROCKEFELLER. All right. I presume you believe that apps directed at kids under 13 are covered by COPPA?

Mr. VLADECK. That is correct.

Senator ROCKEFELLER. According to news reports, apps designed to appeal to kids, one with cartoon characters and games, are collecting information at times without adequate disclosure. Would you agree?

Mr. VLADECK. I believe that is correct.

Senator ROCKEFELLER. Now, COPPA has been a very effective tool to protect children's privacy online. Mr. Vladeck, given the growth in mobile applications, the increasing use of mobile devices by children even to the age of 4, what is the FTC doing to make sure that apps are compliant with COPPA?

Mr. VLADECK. Well, we are doing two things. One is, as I mentioned before, we are looking for good enforcement targets in this space. And we will be bringing other enforcement cases.

Senator ROCKEFELLER. What do you mean by "looking for good enforcement?"

Mr. VLADECK. Cases like Playdom, which involved substantial violations of the act. In Playdom, literally hundreds of thousands of kids were playing these online games. And part of what we do in our enforcement is try to send a clear message to industry.

Playdom was a very big player in this field. It was owned—recently acquired by the Disney Corporation, so——

Senator ROCKEFELLER. OK. So the FTC testified before this committee last year on your plans to review COPPA rules. One of the issues discussed at that hearing was the rules' applicability to the mobile apps. The comment period closed in last July.

Mr. VLADECK. That is correct.

Senator ROCKEFELLER. And so, that is, I think, about a year later. So I am kind of curious as to what you are doing to make up for this lost 10½ months.

Mr. VLADECK. With all respect, the time has not been lost. These raise very difficult public policy issues, and we want to get this right. And so, you can expect something—you know, we hope to get something out in the next couple of months.

Senator ROCKEFELLER. I hear that so often in government. People have to put out rules. They have to put out regulations. We hope to get that out in several months, but in the meantime, everything is OK. I am a bit skeptical.

Mr. VLADECK. I am not saying everything is OK, Mr. Chairman. Please understand that——

Senator ROCKEFELLER. But you implied that you are being active in the meantime, and all I am saying is get the rules out.

Mr. VLADECK. We hear you loud and clear.

Senator ROCKEFELLER. Thank you.

Senator PRYOR. Thank you.

Senator Kerry?

Senator KERRY. Thank you very much, Mr. Chairman.

Mr. Vladeck, thanks for being here.

To what degree is it true that right now, absent some kind of promise to the contrary, any kind of company or a mobile phone or an app operator, hotel, website, whatever it is, that they can do whatever they want with the personal information that they have collected, and the individual would have no right whatsoever to tell them to stop or to control what they are doing with the information?

Mr. VLADECK. Well, if you are asking what the individual could do, that may be a question of State law and Federal law. If you are asking what the Federal Trade Commission can do, our principal tools are deception and unfairness.

In the absence of a privacy policy, it makes things more difficult for us because our jurisdictional hook would be the unfairness prong—generally—would be the unfairness prong of our authority. And while I wouldn't rule out our ability to take enforcement actions in the absence of any commitment through a private policy or any other statement, it would make things more difficult for us.

Senator KERRY. Do you know of a law or do you know of a standard in some state that has been applied——

Mr. VLADECK. I don't know. I have never taken a comprehensive look at that question.

Senator KERRY. You guys have not actually surveyed that to determine what kind of rights people may have?

Mr. VLADECK. When I say "me," I was speaking just for myself. It may well be that our staff has done that. And if so, we would be glad to provide——

Senator KERRY. Could you find out and let us know?

Mr. VLADECK. Yes. I will be glad to provide that to you. Yes, sir.

Senator KERRY. Whether or not you have.

You raised this question of where the FTC can go with respect to an unfair trade practice, which is essentially saying that if somebody makes a promise to the consumer, but they do something other than the promise, you have a right to come in and do something. Absent that, do you have any capacity to assure compliance across the hundreds of thousands of different companies in the country with respect to privacy for consumers?

Mr. VLADECK. We do if the practice is an unfair one under our statute. And——

Senator KERRY. What is the definition of that? What would the standard be that would be applied to that?

Mr. VLADECK. Well, it would have to cause or threaten to cause injury to consumers that the consumers themselves could not avoid and that the cost to consumers would outweigh whatever benefits that might accrue to the——

Senator KERRY. Well, have you made any judgment as to broadly whether or not, in fact, it is unfair, per se, for this information to be given to a third party, for instance?

Mr. VLADECK. We have not made that——

Senator KERRY. Why would that not be something you would want to think about?

Mr. VLADECK. Well, let me digress. We have made that argument, for example, in the data security area. For example, if there is a data security breach and your personal information is shared as a result of the breach, we apply our unfairness standard in those kinds of cases because you have been injured, you could not reasonably avoid it, and the benefits to the company certainly don't outweigh the cost to you.

And that—I am sorry.

Senator KERRY. No, that is all right. I just—unfortunately, time is short. But I want to just try to hone in on some of the things that are sort of out there.

Supposing you have a Government entity and Government information would be a separate committee and a separate set of concerns, but in a private company and a private individual in some kind of right of action, what kind of rights might people have here?

For instance, in a divorce proceeding, could one spouse or the other use information from a third party, or would they have rights to that in some way? Do we know the answer to that?

What about a company against an employee, and the employee has been fired for certain practices in the company and you want a trace on the company's phone? Do they have any—or their phone, either way?

Mr. VLADECK. You have just sort of chronicled all of the reasons why we think geolocation data is so special and so important. Because under State law, those kinds of things may be available, or there may be no inhibition to sharing them.

And largely because of the examples that you have given, we think geolocation data ought to be treated as special data, just as data about children, health, finances, data that deserves special protection.

Senator KERRY. And with respect to Do-Not-Track, Do-Not-Track applies to third party. Is that correct?

Mr. VLADECK. The way we have defined it in our proposal, yes. When you move across websites and you are tracked, that is what we consider to be third-party tracking.

Senator KERRY. So are apps that are operating on iPhones or on Android phones first parties or third parties?

Mr. VLADECK. Well, I think it, again, depends on how the app functions. If you pick up the *New York Times* app on your phone and you are reading the *New York Times,* if you then—you know, if you then click on the Facebook Like button, then it raises difficult questions.

Senator KERRY. But the bottom line is if they are treated as a first party, then Do-Not-Track would not apply any new standard whatsoever with respect to privacy protection for that particular app. Correct?

Mr. VLADECK. That is correct. Right. If you are not moving across websites. But on some apps you can do that, and that is why the implementation of Do-Not-Track for apps, not for mobile browsers, but for apps, raises different implementation questions.

Senator KERRY. That is why, Mr. Chairman, I just wanted to underscore the need for the sort of broader—there are any numbers of reasons, but I think this helps to underscore why you need that basic standard and code of privacy.

And, well, I will come back to that another time, but I thank you for the time.

Senator PRYOR. Thank you, Senator Kerry.

Senator Klobuchar?

STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Thank you very much, Mr. Chairman.

I have a statistic. It is not nearly as sexy as Chairman Rockefeller's statistic that 72 percent of people sleep with their cell phones, something I just can't get over.

But this statistic shows that nearly three-quarters of consumers are uncomfortable with advertising tracking, and 77 percent don't want to share their location data with app owners and developers. And that is why I believe we need some rules of the road. Senator Kerry mentioned the bill that we have been working on.

I also believe that we need to make sure that we are going after bad actors and people who hack in. I am working on a bill with Senator Hatch on cloud computing that we are going to put out shortly.

And the third is that personal choice also plays a role here. Some consumers may be more comfortable with more data sharing than others, but we have to make sure that they are the ones that are able to make that choice. And that gets to my first question here about privacy choices to consumers.

Currently, how simple and clear is the typical privacy policy to the average consumer, Mr. Vladeck?

Mr. VLADECK. Not much, not very.

Senator KLOBUCHAR. OK. And how valuable do you believe a streamlined privacy policy agreement would be when—moving forward, if we try to set some best practices?

Mr. VLADECK. Well, we discuss this in great detail in our privacy report. But to distill it down to its essence, we think that privacy policy, at least those particularly on smartphones, need to be short, clear, and concise. And they ought to be delivered just when the decision about using the app or sharing information is made.

Senator KLOBUCHAR. And that isn't the truth right now?

Mr. VLADECK. That is not generally the way they are delivered at the moment.

Senator KLOBUCHAR. OK. And second, and Senator Kerry was touching on this, but I know one of the most popular things in our household that Congress did was the "do not call" registry many years ago. And now we are looking with Senator Rockefeller at this idea of Do-Not-Track for mobile phones. What kind of feedback have you received from consumers on the Do-Not-Track?

Mr. VLADECK. We have gotten positive response not just from consumers, who overwhelming support a Do-Not-Track feature, but as you may know, both the browser manufacturers and the advertisers are also gravitating to Do-Not-Track.

I think no one—it is hard to argue in favor of a business model that depends on deceiving consumers. And so, I think there is a great deal of movement toward giving consumers easy-to-use, easy-to-find controls over their own data.

Senator KLOBUCHAR. And what do you see as the challenges in implementing Do-Not-Track on mobile devices?

Mr. VLADECK. Well, I think the only challenge, as you put it, is implementation of Do-Not-Track on the apps. On browsers, the technology would be the same. And one of the reasons why we brought on technologists like Ed Felten, who is a Princeton computer science professor, is to help us work through the implementation issues.

Senator KLOBUCHAR. And how does the FTC's proposal differ from what Apple and Google are currently doing with their smartphone operating system?

Mr. VLADECK. On Do-Not-Track? I am sorry.

Senator KLOBUCHAR. On Do-Not-Track.

Mr. VLADECK. Well, they would differ significantly. I mean, the problem that we face now is that there are browsers that are being adapted to essentially try to clear cookies and send out signals to advertisers basically saying, "Don't track us." But until the advertisers agree to be bound by this and sign up in significant numbers, you know, if that doesn't happen, Senator Rockefeller's bill has started the clock.

I think that the business community knows that, at some point, sooner or later there will be a Do-Not-Track requirement. And so, I think they are trying to figure out how to do this.

Senator KLOBUCHAR. OK. And last question, does the FTC currently have the authority that you believe that you need to promulgate regulations in this ever-changing and ever more sophisticated world? And do we need to do anything more here? I mentioned a lot of things that we are looking at with bills, but in terms of just giving you authority.

Mr. VLADECK. Well, let me answer the question in two ways. First is we do not currently have normal APA rulemaking authority. So we do not really have the capacity today to promulgate regulations in this area.

Second, though, I would say our commission has not sought that specific authority from Congress. I can't speak for the commission on that issue.

Senator KLOBUCHAR. All right.

Mr. VLADECK. Thank you.

Senator KLOBUCHAR. Thank you very much.

Senator PRYOR. Thank you.

Senator Blunt?

STATEMENT OF HON. ROY BLUNT, U.S. SENATOR FROM MISSOURI

Senator BLUNT. Thank you, Chairman.

Just two or three questions. One, with Do-Not-Track, how would apps work? For an app to work, don't you have to track?

Mr. VLADECK. There are apps that—when we say track in the mobile——

Senator BLUNT. Maybe apps is too broad a term. But for a lot of apps to work, don't you have to track?

Mr. VLADECK. Well, again, there is a confusion about tracking in the mobile because it takes on two meanings. One is being followed

you as go from one website to another. That is tracking on the Internet.

Senator BLUNT. Right.

Mr. VLADECK. Of course, in the mobile, there is an additional complexity because you can be physically tracked.

Senator BLUNT. I guess that is what I am asking.

Mr. VLADECK. And that is why—I am sorry, that is why I digressed.

Senator BLUNT. But thank you. That helps me to——

Mr. VLADECK. Senator, yes. For many apps that use geolocation data for functionality purposes, you need to enable the geolocation figures on your phone to use that.

Our concern is not with respect to the app developer pulling down geolocation data, for example, to make sure the map function on your phone worked. It is that there are other apps that are pulling down geolocation data which has no relation at all to functionality.

And oftentimes, the consumer is unaware that the geolocation data is being pulled down, or that once it is being pulled down, it is being shared with ad networks, analytic companies, and this ecosystem behind the screen the consumers are unaware of.

Senator BLUNT. In rulemaking, how hard would it be, do you think, to define, to reach that definition to where you are not allowing tracking for some things, but you understand it has to happen for others?

Mr. VLADECK. Well, I think that the litmus test would be functionality. As I just explained, we don't have rulemaking authority in this area. So to the extent there are definitional questions that need to be resolved across the board, industry is going to have to do that, or this body will have to do that.

Senator BLUNT. These questions about employees and divorce cases and things like that, how is this geolocating data retained? Is it retained in a way that you really could go back and sort out with the individual involved not being—agreeing to that, where they had been for some significant period of time or not?

Mr. VLADECK. Well, I mean, there are State law cases involving divorce and other issues in which geolocation data has been subpoenaed from not just the wireless companies, but from other companies and been used in court proceedings. So, yes. The analytic data——

Senator BLUNT. Has been done and can be done is what——

Mr. VLADECK. I believe that is the case, sir.

Senator BLUNT. What about data security breach, something else you mentioned. Is that more likely within the current environment than if you had a lot of privacy signoffs and opt out and all of that sort of thing?

Mr. VLADECK. Well, the Commission has long called for legislation to enhance both the privacy protections, the safeguards companies are required to use when they store sensitive information, such as geolocation data, and to give public notice of breaches.

Now the concern we have is that the more data of this kind, data that is really special because the consequence of disclosure can be serious, the more companies need to protect that data and to safeguard it and make sure that they are not subject to breach. And

so, these two issues are related. The more sensitive data companies collect, the more we ought to require them to put protections in place to safeguard that data.

Senator BLUNT. I guess I will ask the companies this later. But I am wondering how actually individual-specific those are in terms of any collection matrix that the company does, or do they just have a big universe of people that have contact—that have gone to a certain location or something that they then contact that universe?

Mr. VLADECK. Well, I mean, the *Wall Street Journal* did an article on this precise issue a couple of months ago. And the data is so robust that there are now predictive algorithms that you can use to sort of guess where you are going to be next.

So if—and this, of course, is a hypothetical. But suppose you played golf every Wednesday afternoon, you know, and called in sick. It is not inconceivable that, somehow or another, your employer could get that data and decide maybe you shouldn't be golfing every Wednesday.

Senator BLUNT. You know, maybe I need that because I have so far not been able to guess where the Senate is going to be next.

[Laughter.]

Senator BLUNT. So maybe I need to figure out that algorithm that lets me know what we are doing tomorrow.

Thank you, Chairman.

Mr. VLADECK. Thank you so much.

Senator PRYOR. Thank you.

Senator McCaskill?

STATEMENT OF HON. CLAIRE MCCASKILL, U.S. SENATOR FROM MISSOURI

Senator MCCASKILL. Yes. One of the things that seems to be missing from this discussion is that the value that a lot of this activity provides to the consumer. And let me give you one example. The value of being able to locate where this is, is very important to my privacy because they now have the technology that if this gets stolen from me or if it gets left somewhere, I can remotely go and wipe it clean.

That protects my privacy. That is incredibly important to me because, frankly, I don't want people in here.

And so, have you all looked at the value that has come to the consumer both from the robust technology that has been developed and the incredible ability we have to do so many things? The fact that it is free or almost free. I mean, you pay for some apps, and some of those have geolocations. Most of them don't. And what it provides is an amazing Internet experience primarily funded by behavioral marketing, anonymous behavioral marketing.

So what studies have been done to show the benefits? Because I think most consumers—frankly, asking somebody if they want privacy is asking me whether I love my country. Of course, I want privacy.

But we did HIPAA, and I don't think HIPAA has been anything to write home about. I think all of us sign that stupid piece of paper at the doctor's office and don't get much out of it.

So I am trying to make sure that as we go down this road that we are informing the consumer of, yes, there are some things we need to do on privacy, and I am all for some things. But I am not sure the consumer understands now the value they are getting. Have you all talked about that?

Mr. VLADECK. We have. And this was part of the data collection effort we did as part of our privacy review. And I think that, you know, I think there is no disagreement that consumers value tremendously the flexibility and the capacity, the almost unimaginable capacity these phones bring or these tablets bring to our lives. Nobody is suggesting that we turn the clock back.

The question really is, is do we have a system that is more transparent, that helps consumers understand that there are costs as well as benefits? And one of those costs is, you know, you are absolutely correct. The sort of contextual and behavioral advertising is a source of revenue that funds—many apps are free. They are free, but they are supported by the advertising revenue.

Senator MCCASKILL. It is what has made the whole Internet free is behavioral marketing. And that is why I am anxious to know what do you think the new business model will be?

Mr. VLADECK. Well, I think most consumers—and when we talk about Do-Not-Track, we are not talking about an all-or-nothing choice. One of the reasons why the advertisers are so engaged is they have acknowledged for years that they should not be targeting consumers who do not want to see targeted ads. So they are comfortable with the business model in which consumers have choice.

The question is how many consumers are likely to opt out completely? And I think if the choice is rightly explained to consumers, their choice is to get ads that they may be interested in versus ads that are delivered to them at random. I think most consumers would opt for targeted ads, provided that they know that the ads—that the information collected for those ads will not be used—for purposes other than delivering targeted ads.

The whole secondary use issue is an important one, and they will have some control over those ads. So I, for example, don't have to get those pesky Rogaine ads anymore.

[Laughter.]

Mr. VLADECK. And I think that is the kind of choice and control consumers are really looking for.

Senator MCCASKILL. I just want to make sure that we have looked carefully at what the costs are and carefully at what impact it is going to have on the most successful part of our economy in this country.

And I think for us to go down this road and not really be sure that we are going to inform the consumer that some of the benefits that they take for granted right now could very easily go away if we are not very careful and cautious about what we do here.

Let me ask this final question because my time is almost out. Let us assume, for purposes of this discussion, you get all the authority that you may think you need, and you do a lot of rules and regs, and we will fast forward 2 or 3 years because that is how long it will take.

You think that you are going to have the staff to go after the bad guys on this? Do you have currently enough staff to go after the bad guys?

Mr. VLADECK. We currently are very short-staffed. But having said that, we have a very vigorous enforcement agenda in this area.

In the last couple of months, we have brought enormous cases against Playdom, against Google, against Twitter. So, you know, our staff works very hard and are very capable. But we believe that we have the authority——

Senator MCCASKILL. You don't think you need more people to——

Mr. VLADECK. Oh, I need more people.

[Laughter.]

Senator MCCASKILL. Thank you, Mr. Chairman.

Senator PRYOR. Thank you.

Now when I asked my rounds, I still had 2 minutes left on my questions. And what I would like to do is go ahead and finish my questions and then move to the next panel because we have several witnesses who are here and want to speak.

But let me just ask a couple of follow-ups with you, Mr. Vladeck, before I let you go.

One is more of just an open-ended question that I don't even need an answer to today, but it is something we need to think about. And that is when it comes to children, should there be special privacy protections for children?

And I think that is a hard one to practically put that into effect. But it is just something we need to think about, and we would love to have your help on that as we think through it.

Second, this is something I am going to ask the next panel. But if a person removes an app, does any of the software stay on their phone?

Mr. VLADECK. I don't know that answer, and I will have to get back to you.

Senator PRYOR. And I will ask the second panel as well. I just didn't know if you were aware.

And the third thing I had, before I let you go, is I am concerned about in-app purchases. And I know that I have written a letter to the Commission on that. Do you mind just giving us 1 minute on in-app purchases and where you are and where you think the industry is on that?

Mr. VLADECK. Well, we are engaged in a number of nonpublic investigations. I think the simplest way to put it is no parent hands a child a phone with a game expecting to run up a bill of more than a penny or two. And we have, of course, seen parents be presented with bills in the hundreds of dollars. We are quite concerned about that.

We have registered our concerns with both the app manufacturers and everyone else involved in this ecosystem, and that is an issue that we are pursuing.

Senator PRYOR. Great.

I want to thank you for your attendance today and your testimony, and I am certain that some of my colleagues will have more

questions for the record. So we would love for you to work with our staff on getting those back to us, when you can.

Mr. VLADECK. It is our pleasure. Thank you so much.

Senator PRYOR. Thank you.

And what I would like to do now is go ahead and excuse this panel, this witness, and bring up the second panel. And in order to save time, I would like to go ahead and do their very brief introductions as they are getting situated. We have five witnesses on this panel.

We have Bret Taylor, Chief Technology Officer of Facebook. We have Morgan Reed, Executive Director, Association of Competitive Technology. We have Catherine Novelli, the Vice President, Worldwide Government Affairs of Apple Inc. And we also have Alan Davidson—yes, come on up and grab a seat—Alan Davidson, Director of Public Policy for the Americas, Google Inc. And we have Amy Shenkan, President and Chief Operating Officer of Common Sense Media.

So, as the staff is getting them set up, we appreciate you all being here, and we appreciate your testimony. And as I said with the previous panel, your written statements will be made part of the record. So if you want to sort of streamline that and do it in under 5 minutes, I think the Committee would appreciate that.

But why don't we go ahead and start with you, Mr. Taylor? And if you could give us your statement—again, if everyone can keep it to 5 minutes or less, that would be great.

Mr. Taylor?

STATEMENT OF BRET TAYLOR, CHIEF TECHNOLOGY OFFICER, FACEBOOK

Mr. TAYLOR. Thank you, Chairman.

Chairman Rockefeller, Chairman Pryor, Ranking Member Toomey, and members of the Committee, thank you for inviting me to testify today.

Mobile phones and the Internet bring tremendous social and economic benefits. Just a decade ago, most online content was static and accessed through desktops. Today, the Internet is an interactive social experience, defined by a person's connections, interests, and communities.

And thanks to the explosive growth of smartphones and mobile applications, people can access a personalized social Web wherever and whenever they want. With that growth of innovations comes legitimate questions about protecting personal privacy on the web, and we are grateful to have the opportunity to discuss those issues with other stakeholders today.

Everyone has a key role to play in keeping people safe and secure online. Facebook works hard to protect individuals' privacy by giving them control over the information they share and the connections they make.

As Facebook's chief technology officer, these issues are of particular concern to me. We understand that trust is the foundation of the social web. People will stop using Facebook if they lose trust in our services. At the same time, overly restrictive policies can interfere with the public's demand for new and innovative ways to interact.

For Facebook, getting this balance right is a matter of survival. This is why we work to develop privacy safeguards without interfering in people's freedom to share and connect.

I want to address five main points, which are covered in more detail in my written testimony. First, the openness of the Internet is a catalyst for innovation. This openness is what enabled Mark Zuckerberg to launch Facebook from his college dorm room in 2004, and it now allows more than a million third-party developers to offer a nearly infinite variety of services through the Facebook platform.

In addition, the social Web is an engine for jobs, innovation, investment, and economic growth. Big companies and small businesses are hiring individuals to manage their social media outreach strategies. Entrepreneurs are building new business models based on the social web.

But the Internet's open architecture also creates technical challenges for the transfer of data. Facebook is leading the way in developing new technologies to make the social experience more secure.

Second, mobile technology plays an increasingly important role in how people use Facebook and the social web. Facebook has worked to ensure a seamless experience across our Web and mobile services, and over 250 million people access Facebook on their mobile devices every month.

We are one of the few Internet companies to extend our privacy controls to our mobile interfaces, providing the same privacy controls on our mobile applications as we have on our website. If an individual changes his or her privacy settings on their phone, those changes will change their settings on *facebook.com* and every other device that the user may use to access Facebook.

Third, we have built robust privacy protections into *facebook.com* and our mobile offerings. Because each individual's privacy preferences are different, we cannot satisfy people's expectations by adopting a one-size-fits-all approach.

Instead, we strive to create tools and controls that enable individuals to understand how sharing works on Facebook and to choose how broadly or how narrowly they wish to share information at the time they are sharing it. In particular, we use privacy by design practices to ensure that privacy is considered throughout our company and our products.

We are currently testing a new, more transparent privacy policy that communicates privacy in a simple, interactive way. Our contextual controls allow people to easily decide how broadly they want to share a particular piece of information.

Our sophisticated security protections—including one-time passwords, remote logout, and login notifications—are state-of-the-art. And we continually engage with the Facebook community in order to evaluate and improve our services and the privacy safeguards we offer.

Fourth, we work to build trust on the Facebook platform, which enables independent developers to build social experiences on Facebook, as well as other locations around the Internet. We believe that individuals should be empowered to decide whether they

want to engage with some, many, or none of these third-party services.

For this reason, we have created industry-leading tools for transparency and control so that people can understand what data they are sharing and make informed decisions about the applications and websites they decide to use. We also encourage community policing so that individuals, employees, and developers can help us identify possible issues. These features are available across the entire Facebook experience and our mobile applications and on *facebook.com*.

For the independent developers who use the Facebook platform, we expect and we require them to be responsible stewards of the information they obtain. We have robust policies and technology tools to help them embrace this responsibility, and we are always doing more.

Last year, we worked with other industry leaders to build an open standard for authentication that improves security on the Internet. Now that this standard is mature and has broad participation around the industry, we are requiring developers on the Facebook platform to migrate to it. This transition will result in better and more secure relationships between developers and the individuals who use the applications and the websites they build.

Finally, we use our position in the industry to encourage others to play their part in safeguarding the public's trust, whether it is developers, users, browsers, or operating system designers. We also support government efforts to take action against bad actors and highlight important issues like today's hearing.

Everyone has a role to play in building and securing the mobile and online environments that are enriching people's lives each day.

Thank you for the opportunity to testify, and I look forward to answering your questions.

[The prepared statement of Mr. Taylor follows:]

PREPARED STATEMENT OF BRET TAYLOR, CHIEF TECHNOLOGY OFFICER, FACEBOOK

Chairman Rockefeller, Chairman Pryor, Ranking Member Toomey, and members of the Committee, my name is Bret Taylor, and I am the Chief Technology Officer at Facebook. Thank you for inviting me to testify today on privacy issues in the mobile environment. Facebook is committed to providing innovative privacy tools that enable people to control the information they share and the connections they make through our mobile applications, as well as on *facebook.com*. We appreciate the Committee's initiative in holding this hearing today and providing us the opportunity to discuss our efforts to enable people to connect and share in a safe and secure environment.

The explosive growth of smartphones and mobile applications, along with innovations in the way individuals interact and share information, has brought tremendous social and economic benefits. Just a decade ago, few individuals had Internet-enabled mobile phones. Online content was largely static and consumed through desktops. When people interacted, they did so using very limited forms of communication like e-mail and instant messaging. Today, smartphones have become indispensable devices for many people, and the technology that many of us carry in our pockets enables access to a far more personalized and interactive "social web" through which people can choose to share their experiences with friends and receive content that is tailored to them individually.

Facebook develops innovative products and services that facilitate sharing, self-expression, and connectivity. We work hard to protect individuals' privacy by giving them control over the information they share and the connections they make. For Facebook—like other providers of social technologies—getting this balance right is not only the right thing to do, but a matter of survival. Trust is the foundation of the social web, and people will go elsewhere if they lose confidence in our services.

At the same time, Facebook is fundamentally about sharing, and adopting overly restrictive policies will prevent our social features from functioning in the way that individuals expect and demand. Thus, to satisfy people's expectations, we not only need to innovate to create new protections for individuals' information; we also need to innovate to ensure that new protections do not interfere with people's freedom to share and connect. We need to continually evolve our services and the privacy safeguards included in them to respond to the feedback that we receive from the community and as required by law.

In my testimony today, I will address five topics. First, I will describe how the open architecture of the Internet has empowered the innovations of the social Web and is fueling the growth of the economy. I will also explain how this open architecture presents security and privacy challenges to Internet users and the steps we and other companies have taken to address these challenges. Second, I will discuss the growing importance of mobile services at Facebook and how these innovations are driving the social web. Third, I will address the robust privacy protections that we build into *facebook.com* and our mobile offerings. Fourth, I will discuss the infrastructure tools that we provide in order to encourage responsible privacy practices among the independent developers who use our platform. Finally, I will explain how our efforts in advancing security and privacy online must be matched by those of other actors who likewise have an important role in safeguarding the public.

I. The Importance of the Internet's Open Architecture in Fostering Innovation

Facebook provides people with exciting, innovative and free tools for communication and sharing. In addition, through Facebook Platform, Facebook provides a set of tools that enable independent third-party developers to build applications and websites that are more social and people-centered than traditional Web experiences. In both respects, Facebook seeks to build upon the openness of the Internet. The Internet has flourished as a robust zone for innovation and expression because it is an open marketplace in which ideas succeed or fail based on merit. The Department of Commerce recently noted that, "in contrast to the relatively high barriers to entry in traditional media marketplaces, the Internet offers commercial opportunities to an unusually large number of innovators, and the rate of new service offerings and novel business models is quite high." [1] This environment is what enabled Mark Zuckerberg to launch Facebook from his college dorm room in 2004. That same innovative spirit is flourishing on Facebook Platform, which is now used by more than a million third-party developers to offer a nearly infinite variety of tools that enhance individuals' experience both on and off Facebook.

The Internet as it existed at the turn of the millennium was a relatively isolated, passive, and anonymous experience, and few individuals had the ability to access online services through their mobile phones. All visitors to a news site, for example, had the same, one-size-fits-all experience—as if each of them had purchased the same edition of the same newspaper. Thanks to the transformative effects of social technology, people today can enjoy constant connectivity, personalized content, and interactive social experiences across a range of devices. On Facebook, for example, each of the more than 500 million people who visit the site each month has a highly personalized, unique experience—one that provides updates and other content based on the information and activities that the user's own unique circle of friends have shared. The social Web also creates enormous opportunities for anyone with an Internet connection to connect and share with their family, friends, and the world around them. I am proud to say that almost every United States Senator and more than 400 members of the House of Representatives, have Facebook pages that they use to reach their constituents and engage with them on matters of policy and public concern. I am equally proud to highlight that, after the recent tornadoes in the Southeast scattered irreplaceable photographs and other documents far from their owners' homes, one individual created a Facebook page that more than 100,000 people eventually connected with in order to identify and return thousands of items that might otherwise never have been recovered. Further from home, Facebook's photo and video-sharing features enable members of the military to stay connected with their friends and families—to watch their children grow—despite serving thousands of miles away. And, as recent news reports reveal, people around the world have embraced Facebook and other social media as key tools for social engagement.

---

[1] DEP'T OF COMMERCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK 19 (Dec. 16, 2010).

The social Web is also an engine for jobs, innovation, investment, and economic growth. One job-listing site alone includes 31,000 Facebook-related jobs.[2] Small businesses are increasingly relying on social media to generate exposure for their companies, increase sales, and obtain new business partnerships—in a recent survey, two-thirds of small business owners "strongly agreed" that social media was important for their company.[3] The social Web also creates new opportunities for businesses to inform people about their products and services, which is why many companies are now hiring individuals to strategize around social media outreach.[4] At least as important, hundreds of thousands of developers have built businesses by creating applications for the social web. To take just one example, game developer Zynga, creator of the popular Farmville game, plans to hire an additional 700 employees this year and has been valued at $7 billion.[5] And entrepreneurs have only begun to tap into the advancements in productivity and collaboration that social media makes possible, which means that the social Web will continue to transform the economy for years to come.

The open architecture of the Internet makes it a phenomenal catalyst for connectivity, sharing, and economic growth. But that same openness creates technical challenges: what was secure enough for the anonymous Web is not secure enough for the social web. Facebook will continue to develop new technologies that protect individuals' security and privacy on the social web, and time and again we have demonstrated our ability to move quickly to address the challenges associated with harnessing the innovation of the Internet while advancing technology in a way that makes the social experience more secure. I discuss these efforts in more detail below in Sections III and IV.

II. The Role of Mobile Services at Facebook

Over 500 million people now use Facebook's free services to connect and share their information, and more than 250 million of them do so through mobile devices. The proliferation of technology platforms means that individuals are accessing Facebook on multiple devices and in a variety of circumstances—at work, at home, at school, and on the go. Ensuring a seamless experience across all of our web and mobile presences is a tremendous engineering challenge. Whenever we roll out new features, we must consider how they will be implemented on multiple versions of our product: *facebook.com,* our various mobile sites, the iPhone application, the Android application, Facebook for Blackberry, and custom integrations of Facebook on other mobile devices.

Facebook has taken the lead in developing innovative privacy tools to enable individuals using Facebook through mobile devices to share and connect with the people they care about, whenever and wherever best suits them. For example, we recently launched a new version of our mobile website, *m.facebook.com,* that is simpler and works with the capabilities of thousands of different phones. We also introduced *0.facebook.com* as a faster and free way for people to access Facebook around the world, including in locations where connectivity is especially costly and slow. Individuals who access *0.facebook.com* on the networks of our partner mobile service operators can update their status, view their News Feed, comment on posts, send and reply to messages, or write on their friends' Wall—without any data charges. Individuals only pay for data charges when they view photos or when they leave to browse other mobile sites.

Another innovation we rolled out last year was Facebook Places, a feature that allows people to share where they are and the friends they are with in real time from their mobile devices. For example, individuals attending a concert have the option of sharing their location by "checking in" to that place, which lets their friends know where they are. Individuals can also easily see if any of their friends have chosen to check in nearby. Facebook Places supplements existing sharing tools by enabling individuals to connect with each other in real time and in the real world.

A recent report by the Pew Internet & American Life Project found that two-thirds of American mobile phone users take advantage of advanced data features,

---

[2] Shareen Pathak, *The Facebook Job Engine*, FINS (May 16, 2011), *http://it-jobs.fins.com/Articles/SB130514803310615197/The-Facebook-Job-Engine?link=FINS_hp*.

[3] Michael A. Stelzner, 2011 SOCIAL MEDIA MARKETING INDUSTRY REPORT 11, 17–18 (Apr. 2011), *http://www.socialmediaexaminer.com/SocialMediaMarketingReport2011.pdf*.

[4] *See, e.g., Social Media Growth Creates New Job Opportunities,* HERALD & REVIEW, Jan. 4, 2011, *http://www.herald-review.com/news/national/article_5a1ff620-1811-11e0-95b5-001cc4c002e0.html*.

[5] Pathak, *supra* note 3.

such as mobile applications, e-mail and Web access, and text messages.[6] The ubiquity of mobile technology makes it easier than ever for people to tap into the social web, especially for people who may not have access to broadband but do have a mobile phone. Our own internal research shows that people who access Facebook through mobile devices are typically twice as active as other individuals. This increased attention, together with the technological ability to introduce innovative features that utilize mobile capabilities, means that mobile will play an increasingly important role in how people use Facebook and the social Web more generally.

III. Facebook's Commitment to Privacy in Our Product Offerings

As we continue to develop rich services on Facebook, we are guided by our recognition that trust is the foundation of the social web. As the Commerce Department has noted, "[C]onsumer trust—the expectation that personal information that is collected will be used consistently with clearly stated purposes and protected from misuse is fundamental to commercial activities on the Internet." [7]

Facebook builds trust, first and foremost, through the products and services we make available on *facebook.com.* We understand that individuals have widely varying attitudes regarding the sharing of information on Facebook: some people want to share everything with everyone, some want to share far less and with a small audience, and most fall somewhere in between. Because each individual's privacy preferences are different, we cannot satisfy people's expectations by adopting a one-size-fits-all approach.[8] Instead, we strive to create tools and controls that enable individuals to understand how sharing works on Facebook, and to choose how broadly or narrowly they wish to share information. Our commitment to these basic concepts—understanding and control—is evidenced in five specific areas, each of which is a key focus of our business.

Privacy by Design. We have taken several steps to ensure that privacy is being considered throughout our company and products. For example, we have a Chief Privacy Counsel and other dedicated privacy professionals who are involved in and review new services and features from design through launch to ensure that privacy by design practices are incorporated into our product offerings. We also provide privacy and security training to our employees, engage in ongoing review and monitoring of the way data is handled by existing features and applications, and implement rigorous data security practices. Of course, "privacy by design" does not mean "privacy by default"; as services evolve, so do people's expectations of privacy. At Facebook, we believe that providing substantive privacy protections means building a service that allows individuals to control their own social experiences and to decide whether and how they want to share information.

Transparent Policies. Many websites' privacy policies are challenging for people to understand because they are often written for regulators and privacy advocates, not the majority of people who actually use those websites. We believe that privacy policies can and should be more easily understood, which is why we are currently testing a new policy that communicates about privacy in a simpler, more interactive way. We call this "Privacy Policy 2.0." It uses easy-to-understand language, presents information in a layered format so that individuals can quickly zero in on what they want, and incorporates explanatory screenshots, examples, interactive graphics, and videos throughout.

Contextual Control. In its December 2010 *Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, the FTC emphasized that consumers should be "presented with choice about collection and sharing of their data at the time and in the context in which they are making decisions." Facebook agrees. We introduced innovative per-object sharing controls in July 2009 to give people an easy way to indicate how broadly they want to share particular pieces of information. Using the per-object sharing controls, people can designate a unique set of sharing preferences for a particular type of content (such as photos and videos posted by that individual). They can also click on a simple lock icon that appears at the time of publication if they want to customize the audience for a particular photo or video that the individual wishes to share more or less broadly.

---

[6] Kristin Purcell *et al., How Mobile Devices Are Changing Community Information Environments,* PEW INTERNET & AM. LIFE PROJECT, 2 (Mar. 14, 2011), *http://www.pewinternet.org/~/media/Files/Reports/2011/PIP-Local mobile survey.pdf.*

[7] Commerce Report 15.

[8] *See, e.g.,* Mary Madden & Aaron Smith, *Reputation Management and Social Media,* PEW INTERNET & AM. LIFE PROJECT, 29 (May 26, 2010), *http://www.pewinternet.org/Reports/2010/Reputation-Management.aspx* (noting that 65 percent of adult individuals of social networking services have customized the privacy settings on their profile to restrict what they share).

Sophisticated Security Protections. We recently launched a variety of features that enhance people's ability to make decisions about the security of the information they provide. We are the first major site to offer individuals one-time passwords to make it safer to use public computers in places such as hotels, cafes, or airports. If people have concerns about the security of the computer they are using to access Facebook, they can request that a one-time password be texted to their mobile phones. We also enable individuals to see all of their active sessions on the site and to log out of Facebook remotely, which they may want to do if, for example, they access Facebook from a friend's computer and forget to log out. In addition, we encourage people to provide information about the devices that they commonly use to log in to Facebook, which allows them to be notified by e-mail or text message if their account is accessed from an unapproved device so that they can quickly secure their account. Finally, we have long used the secure HTTPS protocol whenever an individual's password or credit card information is being sent to us, and earlier this year we offered individuals the ability to experience Facebook entirely over HTTPS.

Community Engagement. We work hard to obtain feedback from the people who use Facebook, and we consider this input seriously in evaluating and improving our products and services. Indeed, Facebook's efforts to publicly engage on changes to its privacy policy or information sharing practices are virtually unparalleled in the industry. For example, when we propose changes to our privacy policy, we announce them broadly and give individuals the ability to comment on the proposed changes (unless the changes are administrative or required by law). We are the only major online service provider that allows for a vote on the changes if comments reach a pre-set threshold. Time and again, Facebook has shown itself capable of correcting course in response to individual suggestions and we will continue to be responsive to that feedback.

Taken together, these privacy practices help us build and maintain people's trust as we continue to pioneer the new social and connectivity features that people who use Facebook expect and demand. And, because mobile features are increasingly important to the Facebook community, we are leading the industry in innovating around privacy tools available through mobile devices. For example, most of the privacy settings available on the *facebook.com* site are also available to individuals who connect to Facebook through mobile devices. Moreover, these privacy settings are persistent regardless of how the individual chooses to share information. Changes to privacy settings made on our mobile site will remain effective when that individual accesses Facebook through the *facebook.com* website. This enables people to make consistent, real-time decisions about the data they share—no matter where they are or what devices they prefer to use when connecting with their friends and communities.

IV. Promoting Privacy on Facebook Platform

At Facebook, we recognize that we have a responsibility to promote people's privacy interests whenever and however they are accessing Facebook's services. We also understand that Facebook has an important role to play when independent developers build applications and websites that rely on Facebook Platform to create social, personalized experiences. We believe that the best way to build trust while enhancing the openness and connectivity of the social Web is for all members of the Platform ecosystem to embrace their responsibility to be accountable to individuals for protecting privacy.

A. Overview of Facebook Platform

Although we are proud of the pathbreaking features being developed every day at Facebook, we understand that Internet innovation depends on an open architecture in which a multitude of independent developers can develop new services and expand upon existing ones. That understanding is what motivated our decision to launch Facebook Platform in 2007. The Platform functionality allows third-party developers of applications and websites to offer innovative social experiences to individuals on Facebook as well as on other locations around the Internet.

To date, developers have built more than 800,000 games, mobile applications, utilities, and other applications that integrate with the Facebook Platform. To pick just a couple of examples, the Birthday Calendar application allows individuals to track birthdays, anniversaries, and other important dates. The We Read application enables people to share book titles and book reviews with their friends. And on the charitable front, the Causes application provides an online platform for individuals and organizations to raise funds for charitable causes.

The innovation enabled by the Facebook Platform extends to the mobile web. As discussed above, people who use Facebook have the option of sharing location data so that they can tell their friends where they are, see where their friends have

checked in, and discover interesting places nearby. With an individual's express permission, third-party developers can access location data to create a variety of additional social experiences, such as a travel application that gives people the ability to see which of their friends have already been to the place they are visiting, or a conference application that makes it easy for attendees to find colleagues and connect with them.

We are proud of the fact that, in just four short years, Facebook Platform has evolved into a flourishing, open ecosystem where everybody has the opportunity to innovate in a social way. The multitude of applications and websites enabled by Facebook and available through mobile devices is a good example of our commitment to an open architecture for Facebook Platform and the benefits this brings to individuals. The features that we offer on *facebook.com* compete directly with third-party applications and websites that integrate with the Facebook Platform. To pick just one example, Foursquare and Gowalla are popular mobile check-in services that are similar in many respects to Facebook's own Places offering. Subjecting our products to the competitive pressures of the open marketplace helps ensure that we have strong incentives to remain on the cutting edge of innovation, which ultimately benefits the public and the economy as a whole.

B. Tools to Help People Manage Their Relationships with Developers of Applications and Websites

We recognize that the vibrant nature of Facebook Platform creates significant benefits for the public, and we also know that Facebook Platform will only continue to thrive if individuals can build safe and trusted relationships with the applications and websites that they use. Because individuals should be empowered to decide whether they want to engage with some, many, or none of these third-party developers, we have created industry-leading tools for transparency and control so that people can understand what data they are sharing and make informed decisions about the third-party applications and websites that they decide to use. We also make it easy for the Facebook community to identify and report potential areas of concern.

Control. From the time of Facebook Platform's initial launch in 2007, we have made clear to individuals that if they choose to authorize a third-party application or website, the developer will receive information about them, and we have long required developers to obtain only the data they need to operate their application or website. In June 2010, technological innovations allowed us to offer people even more insight into and control over the actions of developers on Facebook Platform: we became the first provider to require developers to obtain "granular data permissions" before accessing individuals' information. Developers using Platform must specifically identify the information they wish to use and request permission from the individual—who retains the ultimate simple choice of whether to share his or her information with that outside developer—and Facebook has deployed technical means to ensure that developers obtain only the information the user has agreed to share. In addition, we make it easy for individuals to revisit their decisions about the applications and websites they have authorized in the past. Users can block applications and websites they no longer want to access their information, and they can also remove certain permissions they have previously granted. Finally, we offer a simple, global opt-out tool. With just one click in the Facebook privacy settings, individuals can opt out of Platform entirely and thereby prevent their information from being shared with any applications or websites.

Transparency. We encourage people to examine the privacy practices of the applications and websites that they use, and we offer tools so that they can easily do so. For example, developers using Platform are required to provide a link to their privacy policy when seeking individuals' permission to access information. In addition, last October, we rolled out an application dashboard to increase visibility into applications' and websites' data handling practices. This audit tool allows individuals to quickly see which applications and websites they have authorized, the permissions they have given to each application or website, and the last time that each application or website accessed their information.

Community Policing. We make it easy for individuals, employees, and developers to communicate with us if they identify a problem with a developer's privacy practices. There is a "Report Application" link on the bottom of each application page so that people can easily convey their concerns about that particular application. Developers, who are often keenly aware of other developers' data handling practices, can and do flag potential issues as well. Our dedicated Platform Operations team, which monitors and enforces Facebook's policies with third-party developers, then follows up on the leads we receive by employing a variety of monitoring, testing, and auditing processes.

Consistent with our commitment to providing a seamless experience across all devices, we have applied these transparency and control principles to the mobile space, despite the engineering challenges associated with communicating on a smaller mobile screen. Individuals who access third-party applications through our mobile offerings are also provided with granular information about what information the application or website seeks to access and asked to specifically authorize the developer's use of that data. In addition, just 2 months after introducing the application dashboard on the *facebook.com* site, we launched a similar mobile application dashboard that allows people to see a detailed view of the information they are sharing with various applications and websites and adjust their settings while on the go.

C. Promoting Best Privacy Practices Among Independent Developers of Applications and Websites

The goal of Facebook Platform is not only to enable developers to build social applications and websites, but also to facilitate direct relationships between people and the social applications and websites they use. At the same time, we expect and require application developers who use Facebook Platform to be responsible stewards of the information they obtain. To this end, we provide clear guidance to developers about how they should protect and secure information obtained from people who use Facebook, and we also build tools to help them fulfill this responsibility.

Policies and Practices. Developers are required to abide by our Statement of Rights and Responsibilities and Platform Policies, which detail developers' responsibilities with respect to the data they obtain. For example, developers may only request the data they need to operate, must honor individuals' requests to delete information, must provide and adhere to a privacy policy that informs individuals about how the application or website handles individual data, and must refrain from selling individuals' data or transferring it to ad networks, data brokers, and other specified entities. In addition, ad networks that developers use to serve ads on applications that run on the Facebook Platform are required to agree to our Platform Terms for Advertising Providers. Among other things, these terms require the ad networks to certify that they do not possess (and will not obtain) any user data received directly or indirectly from Facebook.

Technology Tools for Monitoring and Review. In addition to manual review of specific applications or websites, we also have a series of automated reporting and enforcement tools to quickly identify and respond to potential violations of our policies. Our platform enforcement tool aggregates and displays several metrics concerning the activities of applications and websites on Platform, including how many data requests they are sending, what types of data they are requesting, and whether there have been any complaints or spam reports. We have a separate data access tool that tracks real-time data pulls and rates and provides historical and trend information, giving us insight into applications' or websites' patterns of data access. We also monitor enforcement activity through a dashboard system, which provides a real-time view of identified issues, outstanding enforcement actions, and activity by applications and websites that are under review. These tools enable us to zero in on particular applications and websites that may not be fulfilling their responsibilities, and to work with their developers to ensure that they are taking appropriate measures to protect the information that they obtain.

Continuous Improvement. As innovation fuels further advancements in technology, we implement new tools to help make Facebook Platform a more secure and trusted environment. For example, last year we worked with Yahoo!, Twitter, Google, and others to build OAuth 2.0, an open standard for authentication that improves security on the Internet. Now that OAuth 2.0 is a mature standard with broad participation across the industry, we are requiring developers on Facebook Platform to migrate to the more secure authentication standard. Although the transition presents significant engineering challenges, we believe that this migration is important because it will ultimately result in better and more secure relationships between developers and the individuals who use the applications or websites that they build.

We provide the infrastructure tools described above in order to empower developers to act responsibly when handling individual information, and the vast majority of the applications and websites available on Facebook Platform do so. When we become aware of applications or websites that knowingly break the rules, we take aggressive action to address the policy violation. In appropriate cases, Facebook has required companies to delete data acquired via Platform or banned developers from participating on Platform altogether.

We also have procedures in place to address the possibility of inadvertent data transfers. As I noted above, the open architecture of the Internet is intended to facilitate connectivity and sharing, but that same openness makes it impossible to guarantee the security of every data transfer. We interact regularly with service

providers, security experts, application developers, and other participants in the Internet ecosystem, and when we are alerted to the possibility of a security issue, we act promptly to resolve the problem. For instance, we recently responded quickly after receiving a report from Symantec that so-called "access tokens," which are provided to developers to enable them to obtain the information users have authorized them to obtain, could be inadvertently passed to third parties when developers using a legacy authentication system did not take the necessary technical step to prevent this from occurring. We immediately investigated and, although our investigation found no evidence that this issue resulted in any individual's private information being shared, we took steps—including accelerating the transition to a more secure authentication system—to address the vulnerability Symantec identified before the news became public. As this example highlights, forward-thinking solutions can be achieved when all participants in the digital ecosystem embrace their responsibility to protect individual privacy.

Like all developers who use Facebook Platform, independent developers who work to make the mobile experience more social through integration with the Facebook Platform are required to adhere to our Statement of Rights and Responsibilities and Platform Policies. In addition, we make available software development kits to developers who want to build mobile applications and websites that integrate with the Facebook Platform. Those kits provide tools that help developers build more secure experiences, by incorporating the most advanced and secure technologies available.

V. Numerous Stakeholders Have a Role to Play in Advancing Online Privacy, Safety, and Security

We recognize that Facebook has important responsibilities in advancing people's privacy, safety, and security across the site, our Platform, and the social web. At the same time, others in the ecosystem likewise play an important role in protecting individuals online and in the mobile environment. These include developers, who must establish their own relationships with individuals and live up to the expectations and trust users place in them; browser and operating systems providers, who develop the tools that people use to access the Web and run software and who are perhaps best situated to combat many of the technical challenges associated with the transition from the anonymous Web to the social web; and individuals, who can take security into their own hands through steps such as strong passwords and educating themselves about the practices of the developers with whom they interact.

In fact, the history of advancements in the security of the Internet itself is filled with successes achieved through all affected parties working on tough problems. One example is the development and use of secure socket layers ("SSL") to allow for secure, encrypted Internet communications and data exchanges. SSL was developed by browser vendors largely in response to public demand for a more trustworthy online experience. To realize the full potential of the Internet as a medium for sharing information, developers needed to assure people that their online communications would be secure. The development of secure technologies has led not only to the greater connectivity that characterizes the social Web but also to the explosion of e-commerce and online banking, both of which are crucial drivers of economic growth.

Another advancement that was achieved through the collective efforts of interested parties is the taming of spam e-mail. The late 1990s and early 2000s saw e-mail inboxes and ISP servers overrun by spam, a phenomenon that was not only annoying but also costly to service providers and the public. Although spam remains a serious problem, its worst effects largely have been mitigated through the combined efforts of technology companies' development of sophisticated filtering mechanisms; legislative and regulatory measures such as the Federal CAN–SPAM Act; and the public's continuing demands for action against bad actors. Both of these examples demonstrate how concerted action by various stakeholders in the Internet ecosystem—from site designers and browser vendors to government actors and the public—can contribute to an increasingly secure online environment.

As I explained above, we at Facebook work very hard to build user trust by ensuring transparency and enhancing user control, and by creating a platform that developers can use to build social applications in a safe and secure manner. We also use our position in the industry to encourage others to play their part in building and securing the digital ecosystem. Operating systems and browsers should remain vigilant in identifying and fixing vulnerabilities that could expose data and resolve long-standing design problems inherent in the architecture of the Internet itself. Social sharing networks, including Facebook, should continuously innovate on privacy, educate their users about new privacy features, and enforce their privacy policies with respect to developers who build on social networks' platforms. Developers, in turn, should adhere to our privacy guidelines, publish information about their own

data handling practices, and control third-party access to individual information on their own sites or applications. People who use social sharing services like Facebook should update their passwords, take advantage of safety and security tools and resources, and educate themselves about the policies of websites and social networks they use. And government, too, should play a role, by taking action against bad actors who threaten the trust on which the social Web relies, and, through proceedings such as this hearing, by highlighting the importance of online safety, security, and privacy.

VI. Conclusion

As a facilitator of the social web, we constantly strive to develop better tools that will build trust when individuals access our services through any device. We believe that it is important to enable individuals to make the privacy decisions that are right for them, and to provide infrastructure tools that facilitate trusted relationships between individuals and third-party application developers. By doing so, we are helping to promote the trust that powers the social Web while offering individuals a robust forum to communicate and share information in new and dynamic ways. And we also encourage and support the efforts of other stakeholders in building and securing the mobile and online environments that are enriching people's lives every day.

Thank you for the opportunity to testify today. I look forward to answering any questions you may have.

Senator PRYOR. Thank you.

Mr. Reed?

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

Mr. REED. Thank you, Chairman Pryor, Ranking Member Toomey, and distinguished members of the Committee for the opportunity to speak with you today.

As ACT's Executive Director, I represent over 3,000 developers and small business entrepreneurs, many of whom write apps for smartphones and tablets.

Often when we consider the issues in this grand setting, we do it to look at the impact that it will have on the country at large, and we talk in broad themes and big ideas. But today, I would like to start off a little differently, breaking it down to the smallest of the small, specifically, my pint-sized 5-year-old.

My daughter is learning to speak Chinese. Granted, she is doing it because Dad wants her to. But I let her use an old smartphone. I have loaded on Chinese language learning apps, and she now has games that test her ear, games that help her recognition, and even one that lets her take pictures of a character and gives her a translation.

I have recently seen a demo of an application that will allow her to take a picture of an object and also give her a translation audibly. These are apps that won't make the cut on the desktop computer, if, for no other reason, at least for my 5-year-old will never sit still. Many of the apps were 99 cents. None of them were more than $5.

When she gets a little older, she and I will use Star Walk app, which uses location information to show a real-time movable map of the night sky. Mobile apps like these open up worlds of learning for kids and adults in ways that were unimaginable 5 years ago. And there are thousands of similar stories to mine.

Over 500,000 apps are available on mobile platforms today. Originating less than 4 years ago, the apps economy will grow to $5.8

billion this year. In the next 4 years, that total is expected to reach $37 billion. And if you include services, we expect to hit $50 billion.

This is a remarkable American success story in a time of economic uncertainty. U.S. developers account for the vast majority of apps available in the market today, creating opportunity throughout the country, while also exporting popular programs abroad. Eighty-eight percent of the top 500 apps were written by small businesses, and the vast majority of these, micro-businesses with less than 10 employees.

More importantly, this is not a Silicon Valley phenomenon. In fact, Scott Bedwell developed his series of DJ apps in Bentonville, Arkansas. We have got Marble Burst from ZTak from Thomas, West Virginia. We have got Quick Bins from Moorhead, Minnesota, and we have got Critical Thought from St. Louis, Missouri.

This is the true geographically diverse nature of this new apps economy. And while Apple stores and app stores are helping small businesses grow, the devices and various applications provide the user with tools to protect their personal information.

For the smartphone my daughter uses, I have enabled most of the privacy settings on the device. I have turned off location services. I have restricted her in-app purchases, and I have disabled her ability to add or delete applications. And as she gets older, the features I enable will grow with her maturity.

While the privacy protection in the handset is the place to start, we in the apps community know and are doing more to inform and educate consumers about how we handle their data. Accordingly, ACT has a working group to develop a set of guidelines for mobile application developers to enable them to do a better job in creating privacy policies and also helping them to understand the complexity of privacy regulation.

Most mobile apps collect no information and, therefore, aren't technically required to have a policy, but we feel they should. Not because of regulation, but because the most valuable asset they have is their trust from their customers. A quick peek at the comment section on any mobile app site will show you how quickly an app can lose favor because it failed to meet customer expectations.

Now we don't want anyone to lose sight of the fact that these are hard-working, innovative entrepreneurs who create exciting new products. And ACT is committed to ensuring that they have the tools needed to avoid the pitfalls of data mismanagement. But for those few fraudulent app makers who misuse consumers' personal information, we say throw the book at them.

The FTC's $3 million COPPA fine against Playdom underscored the considerable enforcement measures available. Section V of the FTC Act offers government broad authority to go after bad actors and effectively oversee the marketplace.

While recent events in the media have give a high profile to bad actors in this area, I would urge the Committee to evaluate the considerable enforcement options currently available before creating additional regulatory mechanisms. Too often government intervention in an emerging technology marketplace has unintended consequences that can stunt development.

The last thing we want to do is constrain an industry with tremendous growth, where our country has such a clear competitive

advantage. Let us address bad behavior without threatening this uniquely American apps economy.

Thank you very much.

[The prepared statement of Mr. Reed follows:]

PREPARED STATEMENT OF MORGAN REED, EXECUTIVE DIRECTOR, ASSOCIATION FOR COMPETITIVE TECHNOLOGY

Chairman Pryor, Ranking Member Wicker, and distinguished members of the Committee: My name is Morgan Reed, and I would like to thank you for holding this important hearing on privacy and the growing mobile devices marketplace.

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—and providers of information technology (IT) services. We represent over 3,000 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.

The new mobile apps world has sparked a renaissance in the software industry; small software companies are able to create innovative products and sell them directly to consumers. This is a radical departure from the era of up-front marketing costs, publisher delays, and piracy problems. The emergence of the mobile app market has eliminated the longstanding barriers to entry that our industry battled for the past two decades.

My goal today is to help explain how small business is building this exciting new industry, how what we are doing is helping consumers, and how the very real concerns about privacy must be dealt with holistically, rather than from a technology-specific perspective.

The Smartphone Ecosystem is Creating Jobs and Opportunities in a Tough Economy

The state of the world economy is profoundly unsettled. Questions about job security, healthcare, and foreclosure have become dinner table conversation throughout this country.

In the face of all of this turmoil, there has been a bright spot in economic growth: Sales of smartphones and tablets, such as the iPhone, the HTC Thunderbolt (running Google Android) the Samsung Focus (running Microsoft WP7), the iPad, Xoom and now RIM's Playbook continue to outpace all predictions and are providing a huge growth market in a slumping economy. In fact, nearly one hundred million smartphones were shipped in the first quarter of 2011[1] marking a 79 percent increase in an already fast growing market.[2]

Vendor	1Q11 Shipments	1Q11 Market Share	1Q10 Shipments	1Q10 Market Share	1Q11/1Q10 Change
Nokia	24.2	24.3%	21.5	38.8%	12.6%
Apple	18.7	18.7%	8.7	15.7%	114.4%
Research In Motion	13.9	14.0%	10.6	19.1%	31.1%
Samsung	10.8	10.8%	2.4	4.3%	350.0%
HTC	8.9	8.9%	2.7	4.9%	229.6%
Others	23.2	23.2%	9.5	17.1%	143.7%
Total	**99.6**	**100.0%**	**55.4**	**100.0%**	**79.7%**

Source: IDC Worldwide Quarterly Mobile Phone Tracker, May 5, 2011

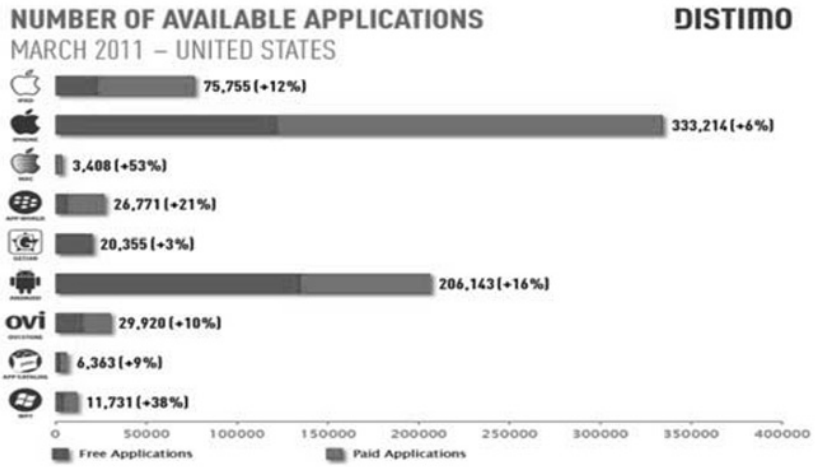
Note: Vendor shipments are branded shipments and exclude OEM sales for all vendors.

In 2008 Apple launched its App Store to provide a place for developers to sell independently developed applications for the iPhone. Since then, over 300,000 new

[1] Mark Kurlyandchik, *IDC: Nokia Remains Top Smartphone Vendor Worldwide,* DailyTech, May 6, 2011.

[2] *Id.*

applications have gone on sale, with billions of applications sold or downloaded. The Android platform has recently exceeded the growth rate seen in the iPhone, totaling more than 200,000 applications, with 10,000 new programs available each month. In 2010 we saw the release of Windows Phone 7, with its own applications store and an entirely unique user interface. Total unique apps across all platforms are expected to exceed 500,000 by the end of 2011.[3]



Possibly the most important thing we have noticed about the new apps world is how it has revolutionized the software development industry. It is nothing less than a rebirth. Startup costs of the modern app developer are a fraction of what they were just 10 years ago. With mobile and Xbox 360 apps, we have seen the return of the small, independent "garage" developer focused on products that can be created and shipped in a matter of months. This new apps-driven model creates a direct bridge between the customer and the developer. Our members tell us that being a developer has not been this exciting since the origins of the personal computer and software industry in the 1970s and 1980s.

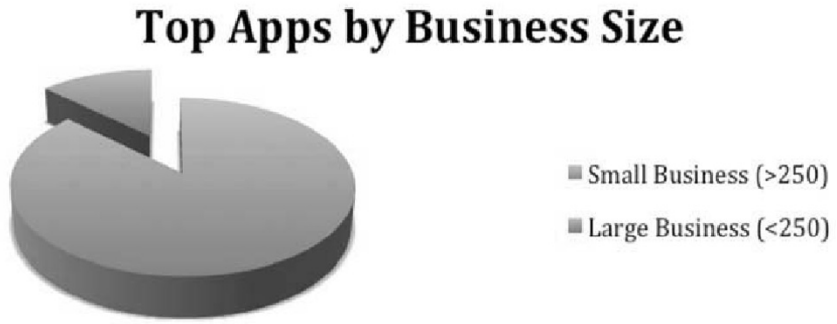
The Mobile App Developer—An Analysis

Apps are overwhelmingly created by small businesses. Of 500 best-selling mobile apps, 88 percent are written by small businesses[4]; and in a majority of cases micro businesses with less than 10 employees.

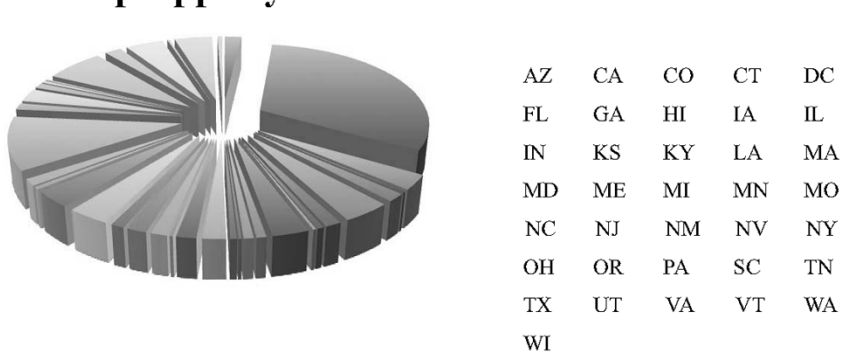
---

[3] *http://d2omthbq56rzfx.cloudfront.net/wp-content/uploads/2011/04/Distimo-survey–201103-app-stores-count.png*.

[4] ACT analysis of top 500 selling apps, some discrepancies exist due to lack of verifiable employment data and apps created by a developer who has significant investment from a larger company. Some apps branded for a larger company are in fact developed by small firms subcontracted to build the application. Sample size of 408 applications, from "top apps" on March 25, 2011.



Second, app developers are not just in California. During the dot-com boom of the 1990s, the majority of growth occurred in Silicon Valley while the rest of the country was not able to reap the direct benefits of the economic boom. The growth of the mobile apps industry has led to job creation all across the United States. While California continues to have a large representation of app developers, nearly 70 percent of the businesses are located outside of the state of California. This new burgeoning industry allows developers to live almost anywhere, including Little Rock, Arkansas and Tupelo, Mississippi.



Third, app development companies have low initial costs but also have the ability to become a highly successful and sustainable business. ACT's members reported development costs ranging from $1,000 to upwards of $1,000,000. Given the wide range of our findings and those of other reports,[5] it is useful to view the cost of mobile app development in tiers.

Tier one represents a simple apps with no real back-end server-based functionality, and can run in the low thousands; this category makes up a significant percentage of all the apps in various mobile stores. They may be single feature programs, vanity apps, or just irreverent apps like iBeer.

Tier two are the apps that provide multiple levels of functionality, often working with data stored in a remote server to provide information/ user generated content, or advanced capabilities like writing and saving specialized documents. This tier runs from $30,000 to $100,000.

Tier three runs from $100,000 on up. This category is for apps that may need to tie into sophisticated inventory management systems, require specialized licenses for content, interface with business critical data bases not just to read, but also write information, and finally, games with immersive environments where art and music costs can be significant.

[5] *http://appmuse.com/appmusing/how-much-does-it-cost-to-develop-a-mobile-app/*.

Understanding the Real Opportunity for Small Business

Mobile App Stores—In a store environment, app developers charge their customers to download applications and/or charge them for purchases they make inside the app. For example, photography app Hipstamatic costs $1.99 to download. If users want additional camera effects (Kodachrome or Holga for instance) they can buy the add-ons in the application.

The exponential growth in app stores during the past few years is unprecedented. Apple was first, launching the iTunes App Store less than 4 years ago, and was soon followed by Nokia, Google, Microsoft, Amazon and others. According to IHS, in 2010 the worldwide market revenue of these app stores in 2010 was $2.15 billion, a 160 percent increase over 2009, and is expected to reach nearly $4 billion this year. Forrester Research estimates that the revenue created from customers buying and downloading apps to smartphones and tablets will reach $38 billion by 2015.

A growing percentage of revenues for app markets are coming from "in-app purchases." According to Xyologic, a company that indexes and analyzes app store data, 40 percent of game downloads are now free titles with in-app purchases. In March, it found there were nearly 100 million downloads of free iPhone games from the App Store.

Yet revenues from app purchases and in-app purchases only represent a part of the overall opportunity for app developers. According to Xyologic, 80.8 percent of all app downloads in the month of March were free. While some of those apps relied on in-app purchasing for revenue, many others were supported by advertising or developed to support other brands and services.

Custom Mobile Development—Additionally, many applications are made available for free by larger companies in order to extend services to mobile devices or as marketing tools. From Citibank's online banking app to Pepsi's "Refresh Project" and Conde Nast's magazine apps, Fortune 1000 companies are increasingly offering mobile apps to their customers and potential customers. While large companies brand these apps, smaller companies with the expertise necessary to build world-class applications under tight deadlines usually build them. These apps represent the majority of the more than 600,000 free apps available across all app markets. This translates into a tremendous number of job-creating opportunities for smaller app development shops. Forrester Research predicts this market to reach $17 billion by 2015.

Mobile Advertising Revenues—Finally, some apps are supported either entirely or partly by advertising revenue. This is an increasingly important model especially as the Android platform grows in marketshare. Some applications charge for downloads and run advertisements inside the app itself. In-app mobile advertising is growing more slowly than revenues from app downloads and in-app purchases, but it is a particularly important revenue model for apps with enormous scale, or "eyeballs." In the games category, which represents around half the app market, the total revenue from in-app advertising was $87 million according to Juniper Research. Juniper expects that to grow to around $900 million by 2015.

The business model of the platform makes a difference in how developers pursue revenue. As shown in an earlier chart, the iOS store has more than 333,000 applications, and nearly 70 percent of those are paid for up front. Google/Android, a company whose entire revenue stream and dominant market position is dependent on advertising, tends to push developers toward the advertising model, with only 30 percent of the 206,000 apps relying on direct payment to the developer.

The Future for Mobile App Developers—Even more important are the opportunities that lay farther ahead. According to a recent Morgan Stanley report,[6] most people haven't yet invested in such technology. True "smartphones" have around 25 percent penetration in the U.S.; in Asia, it may be as low as 6 percent. This represents a pathway for growth leading far into the future.

To understand just how important international sales are to the mobile apps market, one only needs to look at a comparison between the total number of users possessed by a combined AT&T/T-mobile (130 million wireless subscribers)[7] and China's number one wireless carrier, China mobile (584 million subscribers).[8] Even if only 6 percent of China mobile's subscribers become smartphone users—and app purchasers—the market opportunity for U.S. software developers is huge.

---

[6] *http://www.morganstanley.com/institutional/techresearch/pdfs/2SETUP__12142009__RI.pdf*.

[7] *http://www.siouxcityjournal.com/business/local/article__f24b5818-ea11-5f04-b0b0-d7bbd02055b0.html*.

[8] *http://www.wirelessweek.com/News/2011/01/Carriers-Subs-Reach-842M-China-Mobile/*.

Taking Privacy Seriously: ACT Developing Mobile App Privacy Guidelines

This nearly $60 billion opportunity is predicated on an ongoing trust relationship between app developers and consumers, and that is why we take privacy so seriously. Accordingly, ACT has convened a working group of app developers representing the entire swath of the apps ecosystem. Additionally, our working group includes privacy experts and representatives from Privo, one of the four FTC-recognized COPPA Safe Harbors.

The goal of this working group is to provide developers with guidelines that help them to create a privacy policy that is clear, transparent, and enables them to fully utilize the various device platforms that are being created today. We expect our initial guidelines to be available within 30 days and will update them regularly. Additionally, we are working with other groups to build a privacy policy generator for app developers. Such a tool would allow developers to create custom privacy policies that fit the specific requirements of their application. This can remove hurdles for these micro firms, and help them to create simple, easy-to-understand privacy policies that comply with existing law and provide useful guidance to consumers.

Finally, our working group is taking a proactive view of the FTC's Section 5 provisions under COPPA. Although we expect the FTC to come out with rules addressing mobile apps and COPPA very soon, we've chosen not to wait. Instead we are creating our guidelines and advising our members that mobile apps fall under COPPA, and apps developers should make sure that their apps comply with COPPA here in the U.S. and any similar privacy provisions in other countries or jurisdictions. When the FTC's rules are promulgated, we will adjust accordingly, but we always stress that members should err on the side of privacy protection.

Enabling Features While Protecting Privacy

Importance of Location Information for Efficiency—In the lead up to today's hearing, considerable critical attention has been directed at the type of information stored on smartphones. A misunderstood element in the public debate on this data collection is the valuable role location information plays in the underlying functionality of the device—beyond just mapping.

When a smartphone tracks the location of its user, it is making a note to remind itself which access point or cell tower was used there to connect to the Internet. When a user returns to that area, the phone remembers this information. Each day most phone users travel the same route to work or to attend school and then return home to the same place. Keeping this data enables the smartphone to easily find an Internet connection providing efficient, constant online access. This is important for two reasons.

First is battery life. A phone uses a lot of power to search for a cell tower or wireless router. If it constantly needs to search for an Internet connection, it will deplete its battery many times more quickly than if it maintained a constant connection. Customers rate the importance of battery life very highly as a feature in the customer experience, so keeping a charge is an important requirement of the phone. By maintaining a list of frequently visited locations, a smartphone avoids draining its battery in search of data connection points.

Map with Location and Traffic Data

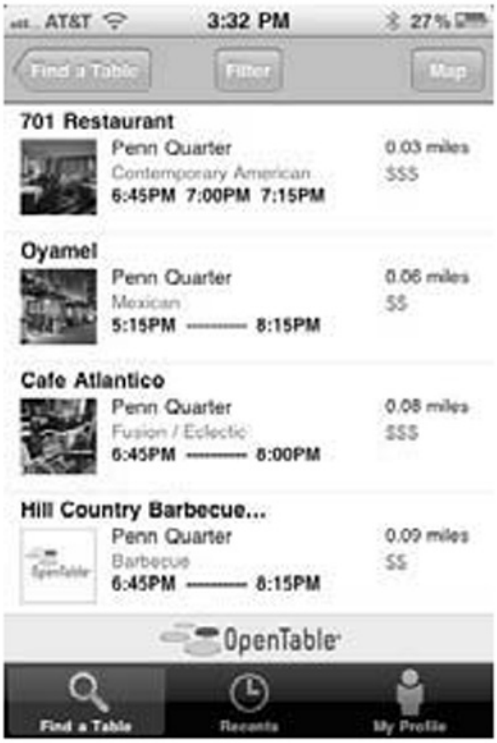
The other reason efficient connectivity matters is spectrum scarcity. The proliferation of smartphones has led to a crowded wireless spectrum, leading to potentially diminishing service quality. Wherever possible, wireless carriers are eager to connect users to wi-fi for faster connection speed and to lessen the burden on wireless networks. Carriers even provide their own wi-fi service for free to customers in densely populated areas to help alleviate the demand for wireless spectrum. By keeping track of the wi-fi and cell tower locations at frequently visited areas, the smartphone can allow users to automatically switch to wi-fi networks to provide constant, high quality Internet connectivity while diminishing the pressures on a crowded spectrum.

Location Information for Consumers—While location data is essential for phones to operate efficiently, consumers also love the smartphone services made possible using location-based technology. Many of the most successful apps or smartphone features have become popular based on knowing exactly where users are at any given time. And that's exactly how customers want it.

Anyone who has owned a smartphone has probably charted their location as a blue dot on their map app. Many also use those same programs to see where the traffic bottlenecks are before starting their evening commute. Some apps use location to help users find the nearest gas station, post office, parking garage, or coffee shop.

The OpenTable app adds location technology to its existing services to allow diners to find open tables at nearby restaurants, read reviews, and make reservations

with a simple tap of the button. Using location information, the app can also provide step-by-step directions to the establishment.



Open Table Reservations

Location services on smartphones have also changed the way we interact socially, creating a market for check-in features to tell your friends and family where you are. Facebook has an app with this feature and, within the last decade, has achieved a market valuation approaching $100 billion. Foursquare, an app which exclusively provides check-in services, has been valued at nearly half a billion dollars.

There is clearly big business opportunity in this marketplace. But location-based services and advertising offer a unique opportunity for Main Street businesses as well. Some apps, like RedLaser, allow users to scan the UPC code of a product and, using the smartphone's location data, find several local retailers nearby where it can be purchased.

Red Laser Bar Code Scan

Meanwhile, a user searching for a particular product or service on their smartphone can receive an ad from a local store based on their current location data. These ads have the benefit of reaching potential customers at the exact time of a purchasing decision and cost far less than the newspaper circulars or the TV ads that big box stores are able to afford.

Similarly, local small businesses can also level the playing field with the national chain stores and Internet retailers through shopping apps like Groupon. This app has 38 million North American subscribers who receive daily discounts at local establishments based on their location data.

While improving the core performance of smartphones, location data is also the building block for apps that users find useful and provide small businesses with opportunities to reach new customers. This data also contains information about the user which they may want to keep private so appropriate safeguards must be in place to ensure it is used in a manner with which consumers are comfortable.

The Smartphone ID Conundrum

Recent news stories have focused on the existence of unique identifiers attached to each smartphone. Known as a UDID number for iPhone and Android ID for Android-based products, this is a number that serves as a unique token for each device. The *Wall Street Journal* article "What They Know—Mobile"[9] made special effort to note the transmission of this number by nearly every single application in

[9] *http://blogs.wsj.com/wtk-mobile/*.

the market. While highlighting the transmission of a "unique identifier" may make for good newsprint, the article unfortunately did not properly explain why developers transmit this number.

In order to help better explain the role this Smart Phone ID (SPID) number plays in the development and maintenance of mobile applications, ACT surveyed developers [10] to find out how they currently used the SPID number. Respondents highlighted three key uses:

- Allows developers to control access to parts of the program without locking the user out completely (*i.e.,* locking achievement levels in games, viewing paid subscriber content);
- Prevents piracy of applications, allows verification of ownership for updates to apps; and
- Allows management of access control for software testing and customer service.

Additionally, developers reported on several benefits to their customers in specific and consumers in general. Most often cited were:

- Working in concert with other stored data, the SPID makes it possible to have applications remember your favorites even when you buy a new phone;
- Helps content providers know when your device is on a wi-fi network instead of 3G, thus allowing them to send you HD or other high bitrate content; and
- Makes it easier to receive updates without verification procedures that annoy customers.

Finally, developers use SPID numbers to interact with third party ad networks; SPIDs are required by many ad networks as part of the terms of service.

At first glance, it would seem to make perfect sense to only allow the SPID to be shared with the app maker itself, but not with third parties. However, in today's world, many different companies work together to provide services to customers. For instance, when shipping a product via FedEx, the sender shares considerable personal information about the recipient with the (third party) shipper including contact information and purchased items. Similarly, small businesses rely on cloud computing to give customers a complete service offering in a cost-effective way. For game developers, a company like OpenFeint offers an easy way to keep track of scores and allows game users to interact with each other, saving app makers thousands of dollars in development time and ongoing infrastructure cost. This service needs to be able to tell devices apart.

Finally, developers felt that the usage restrictions and best practices for SPIDs were well documented, especially on Apple's iOS giving us plenty of advice to app makers on how to properly handle this information.[11]

The key takeaway from this survey is that it is important, and often necessary, to keep devices separate and uniquely identified. Users may own many devices, multiple people may share devices (for example, family members), and others switch devices. Developers have different technical reasons to identify devices, but all come down to the same thing: enhancing the user experience. The developer's focus is in making the user's phone more convenient and useful.

Understanding the Existing Laws and Regulations

Regardless of how data protection is approached, it's critical to note the protections offered under existing Federal and state laws and regulations. In particular, consumer-protection laws currently provide technology-neutral legal standards to address data-privacy and data-security concerns regardless of whether they arise from undisclosed hacking, phishing, inadvertent peer-to-peer "sharing" of sensitive personal files, unauthorized wifi-snooping and art contests seemingly designed to enable the reverse-engineering of children's Social Security numbers.

Currently, the FTC Act gives the FTC broad authority to act against those who misuse data, regardless of the technology used. Specifically, Section 5 of the FTC Act directs the FTC to take action against any business engaging in "deceptive" or "unfair" trade practices.[12]

The FTC's duty to halt deceptive trade practices authorizes the FTC to take law enforcement action not only when a business violates explicit promises to con-

---

[10] ACT April 28 questionnaire to members working on at least one mobile platform. Question: How do you currently use UDID/Android ID in your development process?

[11] *http://developer.apple.com/library/ios/#documentation/uikit/reference/UIDevice__Class/Reference/UIDevice.html*.

[12] 15 U.S.C. § 45.

sumers,[13] such as violations of stated privacy policies or terms of use, but also even when a business makes material omissions to consumers,[14] such as not telling consumers about the sharing of their collected information with third parties.

Similarly, the FTC's duty to halt unfair trade practices authorizes the FTC to take law-enforcement action when business practices cause injuries to consumers that are: substantial; not outweighed by countervailing benefits to consumers and competition; and could not have been reasonably avoided by consumers themselves.[15] For example, the FTC can take action against a business's failure to report a data breach.

Finally, it is critical to understand two points about consumer-protection laws. First, the FTC has real teeth if it finds that a company engaged in "unfair or deceptive practices," including assessing injunctive and civil penalties. Second, state consumer-protection acts grant state Attorneys General even broader substantive and remedial powers than those that Federal law grants to the FTC. As a result, even were resource constraints or agency capture to preclude FTC action in a particular case, 50+ law enforcement agencies would still have broad, technology-neutral authority to protect the privacy and security of consumers' data.

Consequently, the consumer-protection authority of the FTC and state Attorneys General already authorizes and requires these law enforcement agencies to patrol the Internet for companies that might violate their promises to consumers or cause them substantial harm. The FTC recently used such authority to protect consumer privacy by taking action against Google[16] and Chitika[17] for failing to properly handle consumers' information. Both companies now face twenty years of oversight and damage to their brands.

Existing consumer-protection laws thus already authorize both the FTC and state law enforcement agencies to police the entire range of products that connect to the Internet, including mobile devices, and to take action against the bad actors that ignore existing laws and will continue to ignore any future laws. This existing authority also ensures that good actors already have every incentive to behave reasonably and that bad actors have good reason to fear the existing legal consequences of their wrongdoing.

Given the existing authority of the FTC and State Attorneys General, do we need additional regulation? ACT believes this is an open question, but one where consumer privacy protection should not be viewed through a limited, technology-specific lens. Instead, thoughtful, arduous, and considered discussion must take place on the role of personal data in the economy, the true interests of consumers, and the best interaction between citizens and the providers of products and services that use their data.

Avoiding the Patchwork Problem; Dealing with Data Holistically

In periods of great technological change, both new opportunities and new challenges are created. More often than not, however, the seemingly new challenges are merely old issues illuminated under a new light.

Like the dot-com boom before it, the emergence of smartphones and mobile apps have renewed interest in the way corporations and governments collect and share data, most importantly, personal data. Yet, in both cases, these new technologies are simply bringing new light to issues surrounding the collection of personal data that has existed for decades.

There are genuine questions to be asked and considered with respect to the collection and use of personal data. How and when should people be told the data is being collected or when it is being shared? How should they be told? Should people be able to modify data that is collected about themselves? Should people be able to delete data about themselves or otherwise control how it is used? Asking these questions only in the context of smartphones and mobile apps ignores the larger picture. The technology used to collect the data is much less significant than the important questions about the process and behavior of those collecting it.

First, the data collected by apps developers is an almost infinitesimal piece of the global collection of personal data. From credit card companies, to warranty cards, to loyalty programs, companies have been collecting data on their customers long before the Internet or smartphones came around. Not only do other companies collect the same data as smartphone apps, but they have exponentially larger collec-

---

[13] *Id.*

[14] FTC, Policy Statement on Deception (Oct. 14, 1983) available at *http://www.ftc.gov/bcp/policystmt/ad-decept.htm*.

[15] *15 U.S.C.* §45(n); *see also* FTC, Policy Statement on Unfairness (Dec. 17, 1980) available at *http://www.ftc.gov/bcp/policystmt/ad-unfair.htm*.

[16] In the Matter of Google Inc., a corporation, FTC File No. 102 3136.

[17] In the Matter of Chitika, Inc., a corporation, FTC File No. 1023087.

tions of personal data already at their disposal. Information brokers like Epsilon and Google collect, retain, and share far more information than all mobile apps combined.

Even the collection of location data that has been singled out in recent press reports is not unique to smartphones and mobile apps. Standalone commercial GPS providers like TomTom or GPS-based safety services like OnStar collect this information on their users. Your EZ Pass technology for wireless payment of highway tolls also collects and stores location data. More recently, Google has been driving the world's streets eavesdropping on home and business wireless networks to gain the ability to find you even on your home computer or laptop. In nearly every instance, these companies may share that data with third parties.

Isolating and regulating one specific technology is not the answer to the broader questions surrounding the collection and sharing of personal data. Given the enormity of existing data collections and the number of ways it is amassed, focusing exclusively on one technology—particularly the newest and least established—is a symbolic gesture that does not solve the underlying problem, but creates the false sense that the problem has been solved and the need for thoughtful debate and policy consideration is over. Regulatory attention should be focused broadly on behavior and data usage, applying to everyone, regardless of means of collection and sharing.

Finally, regulation that focuses solely on new technology discriminates against small businesses. Whenever we are talking about new, disruptive technologies, we are most often talking about small businesses. Revenue models, customer expectations, and efficiency opportunities are all still emerging, and small businesses are the driving force. Lots of businesses start, a very small number survive, but in the end, we learn what works, and then the large businesses get involved. To stunt the growth of a new, experimental market is to discriminate against the very small businesses on which we rely to lead innovation and growth in the American economy.

Conclusion

The future of the digital marketplace looks bright for small business, so long as the marketplace remains dynamic and competitive. This is a more than $10 billion opportunity for small business across the United States. Barriers to entry in the marketplace are currently low, and our members are very excited about the future—according to ACT's board president, Mike Sax, "Programming is fun again!"

While there are important questions that need to be discussed on personal data collection, retention, and sharing, limiting this question solely to smartphones and mobile apps would be ineffectual and counterproductive.

The use of location information and smartphone IDs are providing immense value to consumers. Whether it's the ability to make dinner reservations or find directions to the nearest hardware store, our members put a value on creating a product that improves the lives of their customers.

Banning the collection of location data would essentially outlaw these beloved consumer apps while doing nothing to address the big questions about data collection and how that data is used. That is why ACT believes that Congress must take a holistic approach to privacy that does not single out any one technology, especially nascent ones. We need to outlaw bad behavior, not good technology. I hope that the committee will continue to focus the spotlight on the contribution small business makes to the future of the digital economy and the way government can do a better job to encourage that productive future. Thank you for your time and consideration on this important topic.

Senator PRYOR. Thank you.

Ms. Novelli?

STATEMENT OF CATHERINE A. NOVELLI, VICE PRESIDENT, WORLDWIDE GOVERNMENT AFFAIRS, APPLE, INC.

Ms. NOVELLI. Good morning, Chairman Pryor, Chairman Rockefeller, and members of the Subcommittee.

My name is Catherine Novelli. I am Vice President for Worldwide Government Affairs for Apple. Thank you for the opportunity to further explain Apple's approach to addressing consumer privacy and protection in the mobile marketplace, an issue we take very seriously, especially as it applies to children.

I would like to use my limited time to emphasize a few key points. First, Apple is deeply committed to protecting the privacy of all our customers. We have adopted a single, comprehensive customer privacy policy for all of our products. This policy is available from a link on every page of Apple's website.

We do not share personally identifiable information with third parties for their marketing purposes without our customers' explicit consent. As explained in more detail in my written testimony, we require all third-party application developers to adhere to specific restrictions protecting our customers' privacy.

Second, Apple has built-in innovative settings and controls to help parents protect their children while using Apple products, both on and offline. These controls are easy to use, password protected, and can be administered on all Mac products, as well as on all of our IOS mobile devices, including the iPhone, iPad, and iPod Touch. These controls can also be enabled quite easily on the iTunes store.

We believe these parental controls are simple and intuitive. They provide parents with the tools they need to flexibly manage their children's activities at various stages of maturity and development in ways parents deem most appropriate. I have provided detailed descriptions and examples in my written testimony.

Third, Apple does not knowingly collect any personal information from children under 13. We state this prominently in our privacy policy. If we learn that we have inadvertently received the personal information of a child under 13, we take immediate steps to delete that information.

We only allow iTunes store accounts for individuals 13 or over. Apple's iAd Network is not providing ads to apps targeted to children, and we reject any developer app that targets minors for data collection.

Fourth, Apple does not track users' locations. Apple has never done so and has no plans to ever do so. In recent weeks, there has been considerable attention given to the manner in which our devices store and use a subset of Apple's anonymized location database of cell towers and Wi-Fi hotspots. The purpose of the database is to allow the device to more quickly and reliably determine a user's location. These concerns are addressed in detail in my written testimony.

I want to reassure you that Apple was never tracking an individual's actual location from the information residing in this cached file on their iPhone. Apple did not have access to the cache on any individual user's iPhone at any time.

Fifth, Apple gives customers of control over collection and use of the location data on all of our devices. Apple has built a master location services switch into our IOS mobile operating system that makes it extremely easy to opt out entirely of location-based services. The user simply switches the location services off in the Setting screen. When the switch is turned off, the device will not collect or transmit location information.

Equally important, Apple does not allow any application to receive device location information without first receiving the user's explicit consent through a simple popup dialogue box. This dialogue box is mandatory and cannot be overridden. Customers may change

their mind and opt out of location services for individual applications at any time by using simple on-off switches. Again, parents can also use controls to password-protect and prevent access by their children to location services.

In closing, let me restate Apple's unwavering commitment to giving our customers clear and transparent notice, choice, and control over their personal information. We believe our products do this in a simple and elegant way.

While Apple has not taken a public position on any specific privacy legislation currently before the Congress, we do strongly agree that any company or organization with access to customers' personal information should give its customers clear and transparent notice, choice, and control over their information. We share the Committee's concerns about the collection and misuse of any customer data, and we are committed to continuing to work with you to address these important issues.

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

[The prepared statement of Ms. Novelli follows:]

PREPARED STATEMENT OF CATHERINE A. NOVELLI, VICE PRESIDENT FOR WORLDWIDE GOVERNMENT AFFAIRS, APPLE INC.

Good morning Chairman Pryor, Ranking Member Wicker, and members of the Subcommittee. My name is Catherine Novelli, and I am Vice President for Worldwide Government Affairs for Apple Inc. On behalf of Apple, I thank you for the opportunity to address this important subject.

Apple's Commitment To Protecting Our Customers' Privacy

As we stated in testimony provided before this Committee last summer, Apple is deeply committed to protecting the privacy of our customers who use Apple mobile devices, including iPhone, iPad and iPod touch.[1] Apple has adopted a single comprehensive privacy policy for all its businesses and products, including the iTunes Store and the App Store. Apple's Privacy Policy, written in easy-to-read language, details what information Apple collects and how Apple and its partners and licensees may use the information. The Policy is available from a link on every page of Apple's website.[2]

Apple takes security precautions—including administrative, technical, and physical measures—to safeguard our customers' personal information against loss, theft, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction. To make sure personal information remains secure, we communicate our privacy policy and security guidelines to Apple employees and strictly enforce privacy safeguards within the company.

We do not share personally identifiable information with third parties for their marketing purposes without consent. We require third-party application developers to agree to specific restrictions protecting our customers' privacy. Moreover, Apple's Safari browser is still the only browser to block cookies from third parties and advertisers by default.

As I will explain in more detail below, Apple is constantly innovating new technology, features and designs to provide our customers with greater privacy protection and the best possible user experience.

We are also deeply committed to meeting our customers' demands for prompt and accurate location-based services. These services offer many benefits to our customers by enhancing convenience and safety for shopping, travel and other activities. To meet these goals, Apple provides easy-to-use tools that allow our consumers to control the collection and use of location data on all our mobile devices. Apple does not track users' locations—Apple has never done so and has no plans to ever do so.

In my testimony today, I would like to reaffirm and amplify Apple's previous privacy testimony before this Committee, while focusing on the following topics of par-

---

[1] Testimony of Dr. Guy "Bud" Tribble of Apple Inc., on Consumer Online Privacy before the U.S. Senate Committee on Commerce, Science, and Transportation, July 27, 2010.

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

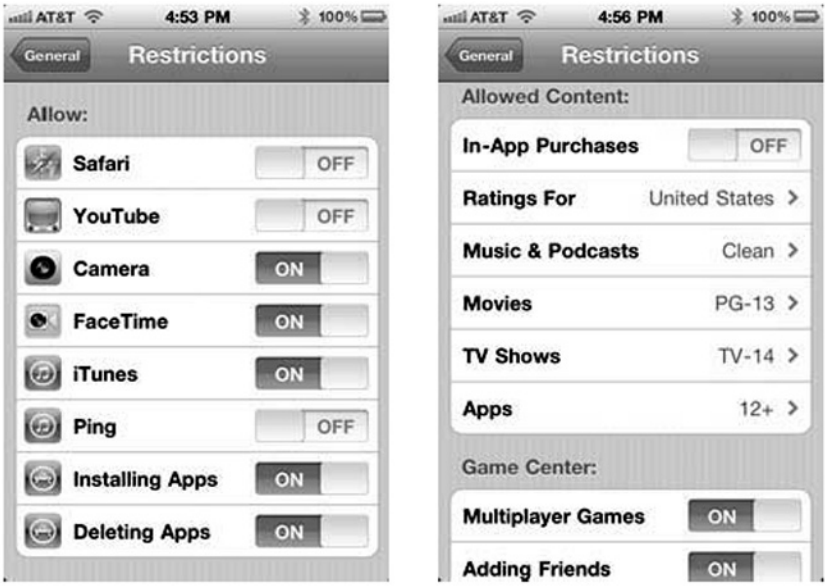
ticular interest for this hearing: (1) Apple's Parental Controls and Restrictions settings; (2) Apple's collection, storage and use of location information on Apple mobile devices; and (3) the use of customer information by third-party applications and the iAd Advertising Network.

I. Apple's Parental Controls and Restrictions Settings

Apple has implemented industry-leading innovative settings and controls to enable parents to protect their children while using Apple products both on and offline. These controls are easy to use, password protected, and can be administered on all Mac OS X products as well as on all of our iOS mobile devices, including iPhone, iPad and iPod Touch. These controls can also be enabled quite easily on the iTunes store.

On any Mac, parents can control which Apps their child can run as well as set age appropriate restrictions for the App Store. Parents also can control with whom their children can exchange e-mails or chat, where they can go online if at all, as well as set time limits as to how long they can be on their computer. There are even settings that enable a parent to prevent their children from using their Mac at all during specific hours, such as during bedtime on school nights. Moreover, these settings provide parents with logs of what their children were doing while using their Macs. These controls are account based, providing a parent with two children, for example, the flexibility to apply different levels of parental controls necessary to manage activities appropriate for their 8 year old versus those appropriate for their 14-year-old teenager—levels which are unlikely to be the same.

On Apple's iOS mobile devices, parents can use the Restrictions settings to prevent their children from accessing specific device features, including Location Services (discussed in detail below), as well as restricting by age level Music, Movies, TV Shows, or Apps, and also prohibiting In-App purchases. When a parent enables these controls, the parent must enter a password (this password is separate from the device password that the Parent may set for their child). Once enabled, a parent can simply tap to switch-on and off access to various features, functions and Apps, even restricting access only to age appropriate content.



EXAMPLE: Above are example screenshots from the iPhone that show restrictions settings that a mother might have set for her young teenage son on his own iPhone. As you can see in this example, this teenager is not permitted to surf the Internet or watch YouTube videos. However, he is permitted to use the iPhone camera and can participate in FaceTime chats with family and friends. His mother also has given him permission to use the iTunes store on his iPhone, but restricted downloads only to age-appropriate music and podcasts, movies, and TV shows.

While this sample teenager also is able to install and delete age-appropriate Apps, his mother has prohibited him from making any In-App Purchases.

We believe these innovative easy-to-use parental controls are simple and intuitive. They provide parents with the tools they need to manage their children's activities at various stages of maturity and development based on the settings they deem appropriate.

Finally, I want to make it clear to the committee that Apple does not knowingly collect any personal information from children under 13. We state this prominently in our Privacy Policy. If we learn that we have inadvertently received the personal information of a child under 13, we take immediate steps to delete that information. Since we don't collect personal information from children under 13, we only allow iTunes store accounts for individuals 13 or over. With respect to our iAd network, our policy is that we don't serve iAds into apps for children. Further, we make it very clear in our App Store Review Guidelines that any App that targets minors for data collection will be rejected.

II. Location Information and Location-Based Services for Mobile Devices

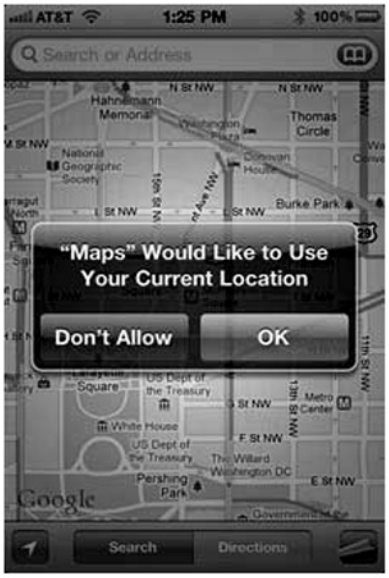
As we stated in our testimony last summer, Apple began providing location-based services in January 2008. These services enable applications that allow customers to perform a wide variety of useful tasks such as getting directions to a particular address from their current location or finding nearby restaurants or stores.

Apple offers location-based services on a variety of mobile devices, including the iPhone 3G, iPhone 3GS, iPhone 4 CDMA and GSM models, iPad Wi-Fi + 3G, iPad 2 Wi-Fi and 3G and, to a more limited extent, older models of the iPhone, the iPad Wi-Fi, and iPod touch.

All of Apple's mobile devices run on Apple's proprietary mobile operating system, iOS. Apple released iOS 4.1 on September 8, 2010. Apple released the current versions, iOS 4.3.3 and 4.2.8 (for the iPhone 4 CDMA model), on May 4, 2011. Currently, iOS 4.3.3 may be run on iPhone 3GS, iPhone 4 GSM model, iPod touch 3rd and 4th generations, iPad, and iPad 2. My testimony focuses on iOS 4.1 and later versions, including the free iOS update Apple released on May 4, 2011.

A. Location-Based Privacy Features

Apple has designed features that enable customers to exercise control over the use of location-based services.



First, as you can see in the iPhone screenshots above, Apple provides its customers with the ability to turn "Off" all location-based service capabilities with a single "On/Off" toggle switch. For mobile devices, the toggle switch is in the "Location Services" menu under "Settings." As described more fully below, when this tog-

gle is switched "Off," (1) iOS will not provide any location information to any applications, including applications that may have previously received consent to use location information; (2) iOS will not collect or geo-tag information about nearby Wi-Fi hotspots or cell towers; and (3) iOS will not upload any location information to Apple from the device.

Second, Apple requires express customer consent when any application requests location-based information for the first time. When an application requests the information, a dialog box appears stating: "[Application] would like to use your current location." The customer is asked: "Don't Allow" or "OK." If the customer clicks on "Don't Allow," iOS will not provide any location-based information to the application. This dialog box is mandatory—neither Apple's applications nor those of third parties are permitted to override the notification.

Third, iOS 4 permits customers to identify individual applications that may not access location-based information, even if Location Services is "On." The Location Services settings menu provides an "On/Off" toggle switch for each application that has requested location-based information. When the switch for a particular application is "Off," no location-based information will be provided to that application.

Fourth, Customers can change their individual application settings at any time. An arrow icon (➤) alerts iOS 4 users that an application is using or has recently used location-based information. This icon will appear real-time for currently running applications and next to the "On/Off" switch for any application that has used location-based information in the past twenty-four hours.

Finally, customers can use Restrictions, also known as Parental Controls, on a mobile device to prevent access to specific features, including Location Services. When a customer enables Restrictions, the customer must enter a passcode (this passcode is separate from the device passcode that the customer may set). If the customer turns Location Services off and selects "Don't Allow Changes," the user of the device cannot turn on Location Services without that passcode.

B. Location Information

1. Crowd-Sourced Data base of Cell Tower Location and Wi-Fi Hotspot Information

Customers want and expect their mobile devices to be able to quickly and reliably determine their current locations in order to provide accurate location-based services. If the device contains a GPS chip, the device can determine its current location using GPS satellite data. But this process can take up to several minutes. Obviously, if the device does not have a GPS chip, no GPS location data will be available.

To provide the high quality products and services that its customers demand, Apple must have access to comprehensive location-based information. To enable Apple mobile devices to respond quickly (or at all, in the case of non-GPS equipped devices or when GPS is not available, such as indoors or in basements) to a customer's request for current location information, Apple maintains a secure database containing information regarding known locations of cell towers and Wi-Fi access points—also referred to as Wi-Fi hotspots. As described in greater detail below, Apple collects from millions of Apple devices anonymous location information for cell towers and Wi-Fi hotspots.[3] From this anonymous information, Apple has been able, over time, to calculate the known locations of many millions of Wi-Fi hot spots and cell towers. Because the basis for this location information is the "crowd" of Apple devices, Apple refers to this as its "crowd-sourced" database.

The crowd-sourced database contains the following information:

> *Cell Tower Information:* Apple collects information about nearby cell towers, such as the location of the tower(s), Cell IDs, and data about the strength of the signal transmitted from the towers. A Cell ID refers to the unique number assigned by a cellular provider to a cell, a defined geographic area covered by a cell tower in a mobile network. Cell IDs do not provide any personal information about mobile phone users located in the cell. Location, Cell ID, and signal strength information is available to anyone with certain commercially available software.
>
> Wi-Fi Access Point Information: Apple collects information about nearby Wi-Fi access points, such as the location of the access point(s), Media Access Control (MAC) addresses, and data about the strength and speed of the signal transmitted by the access point(s). A MAC address (a term that does not refer to Apple products) is a unique number assigned by a manufacturer to a network adapter or network interface card ("NIC"). MAC addresses do not provide any personal information about the owner of the network adapter or NIC. Anyone

[3] During this collection process, iOS does not transmit to Apple any data that is uniquely associated with the device or the customer.

with a wireless network adapter or NIC can identify the MAC address of a Wi-Fi access point. Apple does not collect the user-assigned name of the Wi-Fi access point (known as the "SSID," or service set identifier) or data being transmitted over the Wi-Fi network (known as "payload data").

The crowd-sourced database does not reveal personal information about any customer. An Apple mobile device running Apple's mobile device operating system, iOS, can use the crowd-sourced database to: (1) provide the customer with an approximate location while waiting for the more precise GPS location, (2) find GPS satellites much more quickly, significantly reducing the wait time for the GPS location, and (3) triangulate the device location when GPS is not available (such as indoors or in basements). The device performs all of these calculations in response to a request for location information from an application on the customer's device that has been explicitly approved by the user to obtain the current location, and the device requests from Apple the crowd-sourced database information needed for these calculations.[4]

The crowd-sourced database must be updated continuously to account for, among other things, the ever-changing physical landscape, more innovative uses of mobile technology, and the increasing number of Apple's customers. In collecting and maintaining its crowd-sourced data base, Apple always has taken great care to protect its customers' privacy.

2. Downloading Crowd-Sourced Data To A Mobile Device

To further improve the speed with which the device can calculate location, Apple downloads a subset of the crowd-sourced database content to a local cache on the device. This content describes the known locations of Wi-Fi hotspots[5] and cell towers that the device can "see" and/or that are nearby, as well as nearby cell location area codes,[6] some of which may be more than one hundred miles away. The presence of the local cache on the device enables the device to calculate an initial approximate location before Apple's servers can respond to a request for information from the crowd-sourced database.

One useful way to think of our cell tower and Wi-Fi hotspot database is to compare it to a world map, like the Rand McNally World Atlas, for example. Like a world map, our database of cell towers and Wi-Fi hotspots contains the specific locations of cell towers and Wi-Fi hotspots we have gathered. It doesn't have any information about where any individual person or iPhone is located on that map at any time. The cache on your iPhone is like a series of localized city street maps. When you enter a new area that you haven't been to or haven't been for awhile, we download a subset of the World Atlas—a more localized map of cell towers and Wi-Fi hotspots to your iPhone for the iPhone itself to better assist you. Just as a street map of a city includes all the streets and intersections for many miles around you, it also has the street you are on in addition to all the streets around you, but it doesn't know where you are at any time nor where you go or how often you go there. You use a street map to determine your precise location, relative to fixed points that are identified on the map. Similarly, your iPhone uses the fixed locations of the cell towers and WiFi hotspots to determine its own location relative to those points. Your iPhone, not Apple, determines its actual location without any further contact with Apple once it receives the city maps. Apple has no knowledge of your precise location.

The local cache does not include a log of each time the device was near a particular hotspot or cell tower, and the local cache has never included such a log. For each Wi-Fi hotspot and cell tower, the local cache stores only that hotspot's/cell tower's most recent location information, downloaded from Apple's constantly updated crowd-sourced data base. After a customer installs the free iOS software update (iOS 4.3.3) Apple released on May 4, 2011, iOS will purge records that are older than 7 days, and the cache will be deleted entirely when Location Services is turned off.

---

[4] For devices running the iPhone OS versions 1.1.3 to 3.1, Apple relied on (and still relies on) data bases maintained by Google and Skyhook Wireless ("Skyhook") to provide location-based services. Beginning with the iPhone OS version 3.2 released in April 2010, Apple relies on its own data bases to provide location-based services and for diagnostic purposes.

[5] For each Wi-Fi hotspot, the location information includes that hotspot's MAC address, latitude/longitude coordinates, and associated horizontal accuracy number. For each cell tower, the location information includes the cell tower ID, latitude/longitude coordinates, and associated horizontal accuracy number.

[6] Cell base stations are grouped into "location areas" for network planning purposes, and each location area is assigned a unique "location area code." This "location area code" is broadcast by the cell base stations.

The local cache is protected with iOS security features, but it is not encrypted. Beginning with the next major release of iOS, the operating system will encrypt any local cache of the hotspot and cell tower location information.

Apple issued a free iOS software update on May 4, 2011. Prior to the update, iTunes backed up the local cache (stored in consolidated.db) as part of the normal device backup if there was a syncing relationship between the device and a computer. The iTunes backup, including consolidated.db, may or may not have been encrypted, depending on the customer's settings in iTunes. After the software update, iTunes does not back up the local cache (now stored in cache.db).

When a customer runs certain applications, those applications request location information from iOS. Because of a bug that existed prior to the update, even when Location Services was off, the device would anonymously send the IDs of visible Wi-Fi hotspots and cell towers, without any GPS information, to Apple's servers, Apple's servers would send back the known, crowd-sourced location information for those hotspots and cell towers (and nearby hotspots and cell towers), and the device would cache that information in the consolidated.db file. None of this downloaded crowd-sourced location information or any other location information was provided to or disclosed to the application.

The iOS software update fixed the bug that caused crowd-sourced location information to be downloaded to the device while Location Services was off. iOS will now delete any existing local cache from consolidated.db and, if Location Services is off, (1) Apple will not download any crowd-sourced location information to the device, regardless of whether a specific application requests that information, and (2) iOS will delete any cache of this information stored in cache.db.

3. Collections and Transmissions from Apple Mobile Devices

Apple collects anonymous location information about Wi-Fi hotspots and cell towers from millions of devices to develop and refine Apple's database of crowd-sourced location information. The mobile devices intermittently collect information about Wi-Fi hotspots and cell towers they can "see" and tag that information with the device's current GPS coordinates, *i.e.,* the devices "geo-tag" hotspots and towers.

This collected Wi-Fi hotspot and cell tower information is temporarily saved in a separate table in the local cache; thereafter, that data is extracted from the data base, encrypted, and transmitted—anonymously—to Apple over a Wi-Fi connection every twelve hours (or later if the device does not have Wi-Fi access at that time). Apple's servers use this information to re-calculate and update the known locations of Wi-Fi hotspots and cell towers stored in its crowd-sourced data base. Apple cannot identify the source of this information, and Apple collects and uses this information only to develop and improve the Wi-Fi hotspot and cell tower location information in Apple's crowd-sourced data base. After the device attempts to upload this information to Apple, even if the attempt fails, the information is deleted from the local cache database on the device. In versions of iOS 4.1 or later, moreover, the device will not attempt to collect or upload this anonymous information to Apple unless Location Services is on and the customer has explicitly consented to at least one application's request to use location information.

4. Additional Location Information Collections

If Location Services is on, Apple collects location information from mobile devices under the following four additional circumstances.

First, Apple is collecting anonymous traffic data to build a crowd-sourced automobile traffic database with the goal of providing iPhone users an improved traffic service in the next couple of years. This information is temporarily stored in the local cache on the device, anonymously uploaded to Apple, and then deleted from the device.

Second, Apple collects anonymous diagnostic information from randomly-selected devices to evaluate and improve the performance of its mobile hardware and operating system. For example, Apple may collect information about a dropped cell phone call, including the calculated location of the device when a call was dropped, to help identify and address any cell connection issues. Before any diagnostic information is collected, the customer must provide express consent to Apple. Apple cannot associate this information with a particular customer.

Third, Apple obtains information about the device's location (the latitude/longitude coordinates) when an ad request is made. The device securely transmits this information to the Apple iAd servers, the iAd servers immediately convert the latitude/longitude coordinates to a five-digit zip code, and the iAd servers then discard the coordinates. Apple does not record or store the latitude/longitude coordinates—Apple stores only the zip code. Apple then uses the zip code to select a relevant ad for the customer.

Finally, if a customer has consented to an application's collection and/or use of location information, iOS will provide current location information in response to a request from that application. iOS will provide that customer-approved application with the location of the device only; iOS does not provide applications with direct access to the local cache.

III. Third-Party Applications And The iAd Network

A. Third Party Applications

In July 2008, Apple launched the App Store where customers may shop for and acquire applications offered by third-party developers for the iPhone, iPad and iPod touch. Currently the App Store includes more than 350,000 third-party applications covering a wide variety of areas including news, games, music, travel, health, fitness, education, business, sports, navigation and social networking. Each application includes a description prepared by the developer regarding, among other things, what the application does, when it was posted, and, if applicable, what information the application may collect from the customer.

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

Third-party application developers must register with Apple, pay a fee, and sign a licensing agreement before getting an app on the App Store. The current licensing agreement contains numerous provisions governing the collection and use of user data, device data, and location-based information, including the following:

- Developers and their Applications may not collect user or device data without prior user consent, and then only to provide a service or function that is directly relevant to the use of the Application, or to serve advertising;
- Applications must notify and obtain consent from each customer before location data is collected, transmitted, or otherwise used by developers;
- Developers may not use analytics software in their Applications to collect and send device data to a third party;
- Developers must provide clear and complete information to users regarding their collection, use and disclosure of user or device data (*e.g.,* a description on the App Store or adding a link to the applicable privacy policy).
- Developers must take appropriate steps to protect customers' data from unauthorized use, disclosure or access by third parties.
- If the customer denies or withdraws consent, applications may not collect, transmit, process or utilize the customer's user or device data, including location data;
- Developers must take appropriate steps to protect customers' location-based information from unauthorized use or access;
- Developers must comply with all applicable privacy and data collection laws and regulations regarding the use or transmission of user and device data, including location-based information;
- Applications must not disable, override, or otherwise interfere with Apple-implemented system alerts, display panels, consent panels and the like, including those intended to notify the customer that location-based information is being collected, transmitted, maintained, processed, or used, or intended to obtain consent for such use.

Developers that do not agree to these provisions may not offer applications on the App Store. Apple has the right to terminate our licensing agreement with any developer that fails to comply with any of these provisions. Apple reviews all applications before adding them to the App Store to ensure, for example, that they run properly and do not contain malicious code.

B. The iAd Network

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

As specified clearly in Apple's privacy policy as well as in all relevant Apple device software licensing agreements, customers may opt out of interest-based advertising by visiting the following site from their mobile device: *https://oo.apple.com*. Customers also may opt out of location-based advertising by toggling the device's location-based service capabilities to "Off."

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

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

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

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

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

Senator PRYOR. Thank you.

Mr. Davidson?

STATEMENT OF ALAN DAVIDSON, DIRECTOR OF PUBLIC POLICY, GOOGLE, INC.

Mr. DAVIDSON. Chairman Pryor, Chairman Rockefeller, members of the Subcommittee, my name is Alan Davidson, and I am the Director of Public Policy for Google in North and South America.

Thank you for the opportunity to testify at this important hearing and for the Committee's leadership in helping companies and consumers grapple with these emerging privacy issues.

My message today is simple. As we have heard, mobile services create enormous social and economic benefits, but they will not be used and they cannot succeed without consumer trust. That trust must be based on a sustained effort across our industry to protect user privacy and security, and we are committed to building that trust.

First, a word about technology. Many of us are already experiencing the benefits of mobile and location-based services. Things as simple as getting real-time traffic maps that help aid your commute or finding the closest gas station on your car's GPS.

Thousands of applications use location-based services to help connect consumers and businesses. The U.S. Postal Service offers an app to help users find post offices and mailboxes based on their location. You can find the closest cheeseburger using the Five Guys app, or find your nearby friends on Foursquare.

And the value of location-based services extends far beyond convenience. These services can be lifesavers. Mobile location services can help you find the nearest hospital or police station, or let you know where you can fill a prescription at 1:00 in the morning for a sick child. And that is just the start.

We are now working with partners like the National Center for Missing and Exploited Children to explore how to deliver AMBER Alerts about missing children within seconds to users nearby. And mobile services may soon be able to alert people in the path of a tornado or a tsunami, or guide them to a evacuation route in the event of a hurricane, as I believe, Chairman Pryor, you heard in your hearing in the Homeland Security Committee.

The rapid adoption of these services has been remarkable. For example, on our popular Google Map service, in the past year, 40 percent of our usage has shifted to mobile devices. Every month, over 150 million people now regularly turn to Google Maps on their Android, iPhone, BlackBerry, or other mobile phone.

So mobile services are having growing importance in our economy. According to recent market reports, their potential economic impact is staggering. These services are creating jobs and new businesses, and they are increasing jobs in existing businesses.

But here is the thing. To succeed in the long run, mobile services require consumer trust that is based on strong privacy and security protections. At Google, we focus on privacy protection throughout the life of our products, starting with the initial design. We subscribe to the view that by focusing on the user, all else will follow. So we use information where it provides value to consumers, and we implement strong controls for information sharing, applying the principles of transparency, choice, and security.

When it comes to mobile services, for example, we are extremely sensitive with location information. We have made our mobile location services opt-in only, treating this information with the highest degree of care.

So here is how the opt-in works on Android. When I took my Android phone—actually, this Android phone—out of its box, one of the first screens I saw asked me, in plain language, to affirmatively choose whether or not to share location information with Google. A screen shot of this process is included in our testimony, and it is on the board at the end of the row here.

If a user doesn't choose to opt-in at setup or doesn't go into their settings later to turn it on, the phone will not send any location information back to Google's location servers. If a user does opt-in, all the location data that is sent back to Google's location servers is anonymized, and it is not traceable to a specific user or device. And users can later change their minds and turn it off.

Beyond this, the Android operating system notifies users whenever a third-party application will be given permission to access location information before the user installs the app. That way, the user has the opportunity to cancel the installation if they don't want information collected.

We believe this approach is essential for location services and is a good example of how to handle this kind of sensitive information—highly transparent information for users about what is being collected, opt-in choice before location information is collected, and

high security standards to anonymize and protect information. Our hope is that this becomes a standard for the broader industry.

The strong privacy and security practices I have described are a start. There is more to do. We salute the active role this committee has taken to educate consumers, and we commend what you are doing to bring stakeholders together to develop a comprehensive approach to privacy.

The issues raised are clearly challenging, but finding answers is critical to maintaining consumer trust, protecting innovation, and supporting the rapid economic growth generated by these services. We look forward to continued conversations with the Committee.

Thank you.

[The prepared statement of Mr. Davidson follows:]

PREPARED STATEMENT OF ALAN DAVIDSON, DIRECTOR OF PUBLIC POLICY, GOOGLE INC.

Chairman Pryor, Ranking Member, and members of the Committee:

I am pleased to appear before you this morning to discuss mobile services, online privacy, and the ways that Google protects our users' personal information. My name is Alan Davidson, and I am Google's Director of Public Policy for the Americas. In that capacity, I oversee our public policy operations in the United States, and work closely with our legal, product, and engineering teams to develop and communicate our approach to privacy and security, as well as other issues important to Google and our users.

Google is most well known for our search engine, which is available to Internet users throughout the world. We also make Android, an open operating system for mobile devices that in a few short years has grown from powering one device (introduced in the fall of 2008) to more than 170 devices today, created by 27 manufacturers. We also offer dozens of other popular services, from YouTube to Gmail to Google Earth.

Our business depends on protecting the privacy and security of our users. Without the trust of our users, they will simply switch to competing services, which are always just one click away. For this reason, location sharing on Android devices is strictly opt-in for our users, with clear notice and control. This is the way these services *should* work—with opt-in consent and clear, transparent practices, so consumers can make informed decisions about the location-based services that are so popular.

This is also why we are educating parents and children about online safety, and working with groups like ConnectSafely and Common Sense Media to address the important issues of digital literacy and citizenship, including how to use Google's privacy, security, and family safety tools.

- In my testimony today, I'll focus on three main points:
- Location-based services provide tremendous consumer benefit;
- Google is committed to the highest standards of privacy protection in our services, as demonstrated in our approach to mobile services, content controls, consumer education, advertising, and security; and
- Congress has an important role in helping companies build trust and create appropriate baseline standards for online privacy and security.

I. Location-based services provide tremendous value to consumers

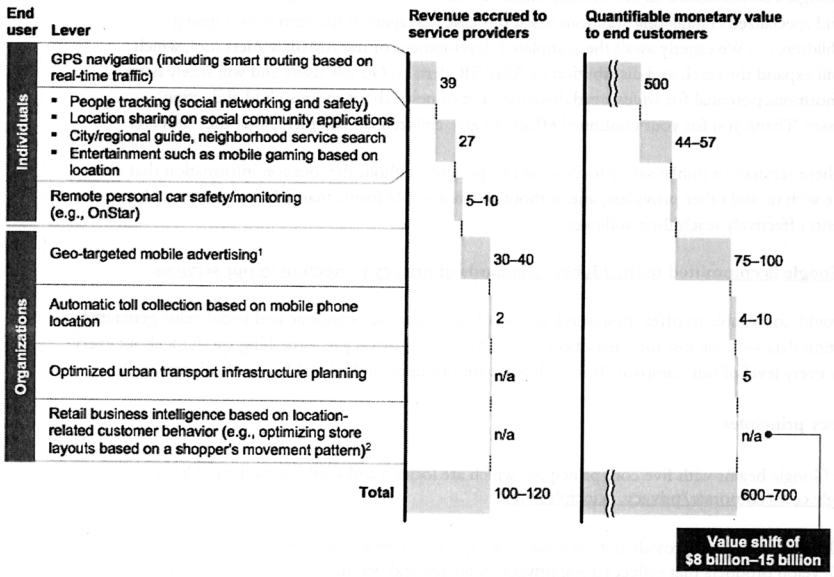
Mobile services are creating enormous economic benefits for our society. A *recent market report* predicts that the mobile applications market will be worth $25 billion by 2015. *McKinsey estimates* that personal location applications will generate as much as $700 billion in consumer value in the next 8 years.

People can use mobile services to get driving directions from their current location, identify a traffic jam and find an alternate route, and look up the next movie time at a nearby theater. Location can even make search results more relevant: If a user searches for "coffee" from a mobile phone, she is more likely to be looking for a nearby café than the Wikipedia entry describing coffee's history. In the last year, a full 40 percent of Google Maps usage was from mobile devices. There are now 150 million active monthly Google Maps for Mobile users on Android, iPhone, BlackBerry, and other mobile platforms in more than 100 countries.

Thousands of other organizations and entrepreneurs offer applications that use location services to provide helpful products. For example, the U.S. Postal Service offers an *application* to help users find nearby post offices and collection boxes, based on their location. If you want a Five Guys burger, their *application* will find a location for you, and even lets you order in advance. Services such as *Yelp* and *Urbanspoon* use location to provide local search results, while applications like *Foursquare* let users find nearby friends who have chosen to share their location.

The value of the major levers increases to more than $800 billion by 2020

$ billion per annum



1 For sizing the value of geo-targeted mobile advertising, service providers are defined as those that sell advertising inventory, e.g., advertising platform providers; customers are defined as the marketers who purchase advertising inventory.
2 Individual retailer will gain top-line increase, which represents a value shift rather than value creation at macro-level.

Source: McKinsey Global Institute analysis.

Mobile location data can even save lives. In crisis situations, people now turn to the Internet to find information. Within a few hours of the Japan earthquake, for example, Google saw a massive spike in search queries originating from Hawaii related to "tsunami." We placed a location-based alert on the Google homepage for tsunami alerts in the Pacific and ran similar announcements across Google News, Maps, and other services. In cases like the Japanese tsunami or the recent tornadoes in the U.S., a targeted mobile alert from a provider like Google, or from a public enhanced 911 service, may help increase citizens' chances of getting out of harm's way.

Other emergency notifications like AMBER alerts can be improved using location data, too. In the past, a parent's best hope of finding a missing child might have been a picture on a milk carton. Google works with the National Center for Missing and Exploited Children (NCMEC) in an ongoing partnership to develop technology solutions that help them achieve their mission. Today, modern tools and information can make NCMEC's AMBER alerts more effective and efficient through location-based targeting—within seconds of the first report, an AMBER alert could be distributed to all users within one-mile of the incident. As Ernie Allen, NCMEC's President and CEO, wrote last week:

> Google's contributions to our Missing Child Division have also been significant. Your tools and specialized engineering solutions assist our case managers in the search for missing children. . . . We eagerly await the completed development of the AMBER Alert tool, which will expand the reach and distribution of AMBER alerts to Google users and will surely have enormous potential for widespread dissemination of news about serious child abduction cases. Thank you for your continued efforts to give children the safer lives that they deserve.

None of these services or public safety tools would be possible without the location information that our users share with us and other providers, and without the mobile platforms that help businesses and governments effectively reach their audiences.

II. Google is committed to the highest standards of privacy protection in our services

Google would not be able to offer these services—or help create the economic and social value generated from location data—if we lost the trust of our users. At Google, privacy is something we think about every day across every level of our company. It is both good for our users and critical for our business.

Our privacy principles

Privacy at Google begins with five core principles, which are located and available to the public at *www.google.com/corporate/privacy_principles.html*:

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

First, as with every aspect of our products, we follow the axiom of "focus on the user and all else will follow." We are committed to using information only where we can provide value to our users. *We never sell our users' personally identifiable information.* This is simply not our business model.

Second, we aim to build privacy and security into our products and practices from the ground up. From the design phase through launch, we consider a product's impact on our users' privacy. And we don't stop at launch; we continue to innovate and iterate as we learn more from users.

Our last three principles lay out our substantive approach to privacy: We are committed to *transparency, user control,* and *security*.

Internal process and controls

Google also reflects these principles in our development process and employee training. As we *recently explained,* we have begun to implement even stronger internal privacy controls with a focus on people, training, and compliance.

All this process is aimed at ensuring that products match our philosophy and avoid mistakes that jeopardize user trust—like the launch of *Google Buzz,* which fell short of our standards for transparency and user control. To help make sure we live up to this promise, we entered into a consent decree with the Federal Trade Commission this year, under which we'll receive an independent review of our privacy procedures every 2 years. In addition, we'll ask users to give us affirmative consent before we change how we share their personal information.

Products reflecting principles: Opt-in location controls on Android

We understand location information is sensitive. So our approach to location data is simple: Opt-in consent and clear notice are required for collection and use of location information on Android.

We don't collect any location information—any at all—through our location services on Android devices unless the user specifically chooses to share this information with Google. We also give users clear notice and control; the set-up process explicitly asks users to "allow Google's location service to collect anonymous location data." And even after the set-up process, users can easily turn off location sharing with Google at any time they wish.

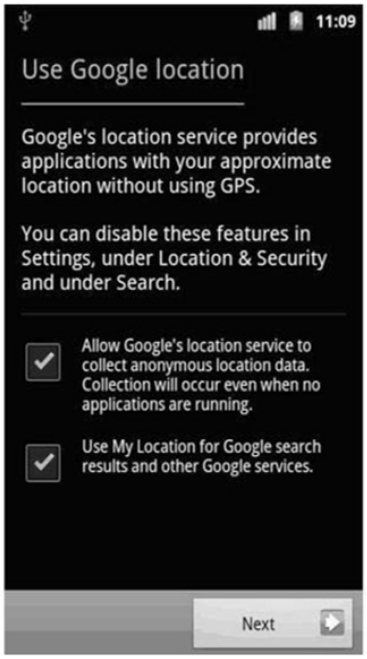
The location services in our Android operating system embody the transparency and control principles that we use to guide our privacy process. We hope that this will be a standard for the industry.

Google is also very careful about how we use and store the data that is generated by these services. The location information sent to Google servers when users opt in to location services on Android is anonymized and stored in the aggregate. It's not tied or traceable to a specific user. The collected information is stored with a hashed version of an anonymous token, and that hashed token is deleted after approximately one week. A small amount of location information regarding nearby Wi-Fi access points and cell towers is kept on the Android device to help the user continue to enjoy the service when no server connection is available and to improve speed and battery life.

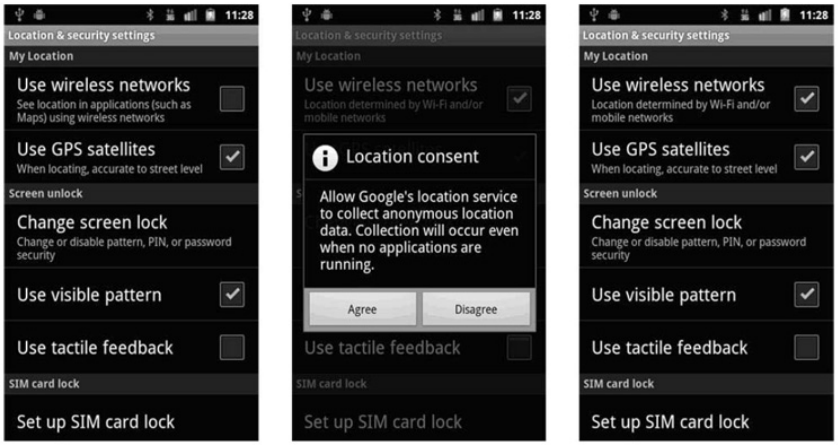
In order to provide these location services, many companies detect nearby, publicly available signals from Wi-Fi access points and cell towers and use this data

to quickly approximate a rough position, even while they may be working on a more precise GPS-based location. This can be done by using information that is publicly broadcast (for example, that list of Wi-Fi access points you see when you use the "join network" option on your computer). Companies like Skyhook Wireless and Navizon compile such information and license the data to many industry leaders.

Google has a similar location service called the Google Location Server—an Internet database that uses Wi-Fi access points and cell towers to determine an estimated location and that uses GPS information to estimate road traffic. Device manufacturers can license the Network Location Provider application for Android from Google. This Network Location Provider is turned off by default. It can be turned on by the user during the phone's initial setup or in the device settings.



The Network Location Provider is off by default. The user can opt-in and turn on location services during the initial setup flow.



The user can opt-in to turn on the Network Location Provider on their Android phone from within the device settings.

The Android operating system is built on openness, with the goal of encouraging developers to innovate. With this principle in mind, Google does not decide which applications can access location or other user information from the device. Instead, the Android operating system uses a permissions model in which the user is automatically informed of certain types of information an application will be able to access. The user may choose to trust the application by completing the installation or the user may choose to cancel the installation. An application can only access the device's GPS location or the device's network location if it displays a notice for this permission to the user at time of installation.

When Google creates an Android application, like Google Maps for mobile devices, Google is responsible for how the application collects and handles data and for the privacy disclosures made to users, and generally applies the *Google Mobile Terms of Service* and the *Google Mobile Privacy Policy.* These privacy policies are also clearly displayed to the user when the user first signs into the Android device.

When an Android application is not developed by Google, the application developer bears the responsibility for its design and its use of data. Google does not and cannot control the behavior of third party applications, or how they handle location information and other user information that the third party application obtains from the device. Google does strongly encourage application developers to use best practices as described in this *Google blog post.*

How our products reflect our principles: Parental controls and family safety

While Google does not offer services directed at children, we try to provide families with the tools and education to ensure a positive and safe experience on our services. In addition to our work with NCMEC and others to protect children, our major consumer education initiatives include:

- *Android Market content ratings.* The content rating system is a new feature of Android Market that requires developers to rate their apps in one of four categories, in accordance with our *guidelines:* Everyone, Low-, Medium-, or High-Maturity. Developers are responsible for rating the apps, and if users come across incorrectly rated apps, they can flag them for review.
- *SafeSearch on Mobile.* Just as with Google Web Search on desktop, Google's SafeSearch filter is accessible on mobile for users who search on a mobile browser. SafeSearch uses advanced technology to block sexually explicit images and text from search results. Users can customize and lock their SafeSearch settings to "Strict" or "Moderate" by clicking on the "Settings" link to the top right corner of the homepage on *Google.com*.
- *Digital Literacy initiative.* To help educate families about responsible Internet use, we developed a *curriculum* with iKeepSafe that teaches teens to recognize online risks, investigate and determine the reliability of websites, and avoid scams. We've sponsored a tour that iKeepSafe is taking across the country to bring the curriculum into local communities and classrooms.
- *Family Safety Center.* In cooperation with the Federal Trade Commission's OnGuardOnline initiative and other child safety advocates and experts, we built a one-stop shop for families, available at *www.google.com/familysafety,* to provide step-by-step instructions for using safety tools built into Google products and other best practices for families to consider. In response to popular requests, we've added a section about *managing geolocation features on mobile phones*.
- *Net Safety Tips on the Go app.* The Internet Education Foundation, in partnership with Google and others, *created an app* to help users keep up with online privacy, safety, and security issues on your Android phone. It provides quick, practical, friendly advice for you and your family. The tips, developed by leading online safety organizations, cover important issues like mobile privacy and safety, sexting and cyberbullying, social networking safety, and avoiding identity theft.

How our products reflect our principles: Advertising and privacy

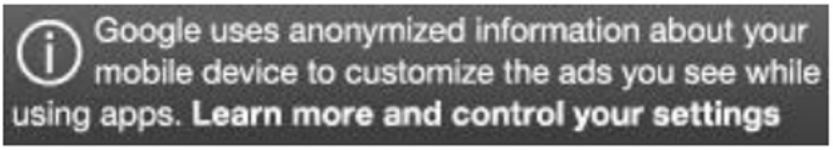
John Wanamaker, considered by some to be the father of modern advertising, once remarked that "half the money I spend on advertising is wasted; the trouble is I don't know which half." Google's advertising products are aimed at eliminating that wasted half, bringing data-driven efficiency to advertising. But as we work to bring more relevant and useful ads to our users, we continually seek to preserve transparency and user control over the information used in our ad system.

Google was not the first to offer interest-based advertising (known as IBA) online, but when we launched IBA, in March 2009, we included a number of groundbreaking privacy features. Google's interest-based ads contain notice in the actual advertisement indicating that it is a Google ad. The in-ad notice is linked to information about IBA, including our Ads Preferences Manager, which allows users to change the interest categories used to target ads, or to opt-out of interest-based advertising altogether. Note that we do not serve interest-based ads based on sensitive interest categories such as health status or categories relating to kids. We are also participating in the *industry-wide ad targeting notice and opt-out program*.

We have seen that for every visitor that opts out of IBA on this page, seven users view or edit their settings and choose to remain opted in. We take from this that online users appreciate transparency and control, and become more comfortable with data collection and use when we offer it on their terms and in full view.

Recently, discussions about online ad targeting have centered on the ability of users to indicate a desire to opt out of this profiling and targeting by all online providers—sometimes called Do Not Track. In January, Google sought to further encourage consistency and ease of control over online targeting by launching the *Keep My Opt-Outs* Chrome extension, which enables all providers participating in ever-expanding industry self-regulatory programs to make their IBA opt outs *permanent* via a simple browser-based mechanism. As new opt outs come online, we will automatically update this extension to keep users up to date. In the first few months, more than 100,000 users have already installed and are using the extension. We even released this tool on an *open-source* basis so that other developers can examine, assess, enhance, or even extend the code's capabilities. Additionally, we are developing versions of Keep My Opt Outs that work on other major browsers.

Just last month, we extended our advertising privacy approach to our mobile application ad networks. These networks help mobile app developers make money from their products. For these ad systems, we have created a user-friendly solution involving anonymization, user control, and user notice. First, Google performs a one-way, non-reversible hashing of a device identifier to create an anonymous ID specifically for ad serving. Second, for both Android and iPhone users we give consumers an easy way to opt out the use of their device identifier by Google's advertising services altogether. Third, we are notifying all users of how we customize ads and their opt-out controls with clear notice as you see here.



Because the mobile application interfaces are more limited, we chose to rotate full-size privacy notices in with other advertisements, rather than use an icon, which is hard to see or click on the smaller mobile screen.

How our products reflect our principles: Security through encryption and two-step verification

Along with transparency and user control, strong security for users of Google's services to protect against hackers and data breach is vital.

For example, Google was the first (and still only) major webmail provider to offer session-wide secure socket layer (SSL) encryption *by default*. Usually recognized by a Web address starting with "https" or by a "lock" icon, SSL encryption is used for online banking and other secure transactions. Users can also encrypt search. Just type "*https://encrypted.google.com*" into your browser to encrypt your search queries and results. We hope other companies will soon join our lead.

In March of last year Google introduced a system to notify users about suspicious activities associated with their accounts. By automatically matching a user's IP address to broad geographical locations, Google can help detect anomalous behavior, such as a log-in appearing to come from one continent only a few hours after the same account holder logged in from a different continent. Thus, someone whose Gmail account may have been compromised will be notified and given the opportunity to change her password, protecting herself and her contacts.

Finally, we recently released *2-step verification* for consumer Gmail accounts, which allows users who are concerned about the security of their account to use a password plus a unique code generated by a mobile phone to sign in. It's an extra step, but it's one that significantly improves the security of a Google Account. Now, if someone steals or guesses a Gmail user's password, the potential hijacker still cannot sign in to the user's account because the hijacker does not have the user's phone. We are already hearing stories from our users about how this extra layer of security has protected them from phishing attacks or unauthorized access.

III. Congress should act to build trust and create appropriate baseline standards

Congress has a vital role to play in encouraging responsible privacy and security practices, both by bringing attention to these issues and through legislation where appropriate.

The first step Congress can take, and one on which we can all find common ground, is the need for basic "digital citizenship" education for parents, children, teens, and all consumers. Digital skills are essential life skills in a 21st century economy, including understanding basic technical concepts like how to create a safe password and avoid online scams, to critical thinking such as evaluating whether information on a blog is reliable or not. It is crucial that Congress and providers work together to create resources for programs that address these issues and promote them to all consumers, particularly parents and educators.

A second area for careful consideration is legislation. Google supports the development of comprehensive, baseline privacy framework that can ensure broad-based user trust and that will support continued innovation. We salute the work of Senators Kerry and McCain to develop a comprehensive approach to this issue, based on the same principles of transparency, control, and security we apply to our own services. We look forward to continued conversations about this bill as it evolves.

Key considerations for any comprehensive approach to privacy include:

- *Even-handed application.* A pro-innovation privacy framework must apply even-handedly to all personal data regardless of source or means of collection. Thus, offline and online data collection and processing should, where reasonable, involve similar data protection obligations.
- *Recognition of benefits and costs.* As with any regulatory policy, it is appropriate to examine the benefits and costs of legislating in this area, including explicit attention to actual harm to users and compliance costs.
- *Consistency across jurisdictions.* Generally, Internet users neither expect nor want different baseline privacy rules based on the local jurisdiction in which they or the provider reside. Moreover, in many instances, strict compliance with differing privacy protocols would actually diminish consumer privacy, since it would require Internet companies to know where consumers are located at any given time.

By the same token, in general we do not support a continued "siloed" approach to privacy law. While much of today's debate centers on location information and "Do Not Track" advertising privacy proposals, providers and consumers need a comprehensive approach that will set consistent, baseline principles for these issues and those to come in the future. Otherwise, this Committee and others will be returning term after term to address the latest new technology fad.

Moreover, industry response to the advertising privacy issue has been encouraging. In a few short months, all major browser companies have introduced new controls, and the advertising and online publishing industries have come together to announce uniform standards for notice and control over targeted ads.

We can, however, suggest two concrete areas where Congress can act immediately to strengthen Americans' privacy protections and provide consistency for providers.

Congress should promote uniform, reasonable security principles, including data breach notification procedures. We pride ourselves at Google for industry-leading security features, including the use of encryption for our search and Gmail services. But we need help from the government to ensure that the bad acts of criminal hackers or inadequate security on the part of other companies does not undermine con-

sumer trust for all services. Moreover, the patchwork of state law in this area leads to confusion and unnecessary cost.

In addition, the Electronic Communications Privacy Act, the U.S. law governing government access to stored communications, is outdated and out of step with what is reasonably expected by those who use cloud computing services. ECPA worked well for many years, and much of it remains vibrant and relevant. In significant places, however, a large gap has grown between the technological assumptions made in ECPA and the reality of how the Internet works today, leaving us in some circumstances with complex and baffling rules that are both difficult to explain to users and difficult to apply.

As part of the *Digital Due Process coalition,* we are working to address this issue. The Digital Due Process coalition includes members ranging from AT&T to Google to Americans for Tax Reform to the ACLU. It has put forward common sense principles that are designed to update ECPA, while ensuring that government has the legal tools needed to enforce the laws.

Particularly relevant to today's hearing, the coalition seeks to:

- *Create a consistent process for compelled access to data stored online.* Treat private communications and documents stored online the same as if they were stored at home and require a uniform process before compelling a service provider to access and disclose the information.
- *Create a stronger process for compelled access to location information.* Create a clear, strong process with heightened standards for government access to information regarding the location of an individual's mobile device.

Advances in technology rely not just on the smart engineers who create the new services, but also on smart laws that provide the critical legal underpinning for continued innovation and adoption of the technology. We hope to work with this Committee and with Congress as a whole to strengthen these legal protections for individuals and businesses.

* * *

Google appreciates the efforts of this subcommittee to address the critical privacy and security issues facing consumers. We look forward to working with you, and to answering any questions you might have about our efforts.

Thank you.

Senator PRYOR. Thank you.

Ms. Shenkan?

STATEMENT OF AMY GUGGENHEIM SHENKAN, PRESIDENT AND CHIEF OPERATING OFFICER, COMMON SENSE MEDIA

Ms. SHENKAN. Good morning, Mr. Chairman, members of the Committee, and thank you for this opportunity to discuss the crucial issue of protecting consumer privacy in this marketplace.

The hearing is timely, and the stakes are high, especially for our nation's kids. I want to talk about two things today. Why is privacy such an important issue? And what is the Common Sense Media position on what we must do about it?

So why is this so important? Let me start by saying that Common Sense Media embraces media and technology. One of our founding beliefs is that we love media, but we and the millions of parents who use our resources are increasingly worried about threats to children's privacy in a rapidly changing mobile and digital world.

Eighty-five percent of parents we polled said they are more concerned about privacy than they were 5 years ago. Let me also preface by saying that Common Sense Media understands and appreciates the Internet economy and the sheer brilliance of what these companies have invented.

We live and work in Silicon Valley. That is why it is so jarring to hear their "can't do" attitude when it comes to inventing techno-

logical solutions to protect kids. We get half measures after the fact, and then they only offer partial solutions. They can do better. We know it. And we believe they know it.

Parents and kids are rightly concerned. So why do we worry? Two reasons. First, kids live their lives online. Kids don't just access content anymore. They create it. Our kids are growing up in public.

Many of the people in this room can attest to how hard it is to be a public figure. Imagine if you are only 13 and had an unflattering picture of you spread across the web, as has happened to hundreds of kids in high schools across the country. Seven and a half million kids under 13 are on Facebook, and millions more teens.

Second, we are also seeing too many examples of how our privacy is not protected in this world. We all know that Sony just experienced a security breach, which exposed personal data of more than 100 million—100 million—of its online video game users. And the list goes on.

This hearing is specifically around mobile, and for good reason. The mobile world puts all the privacy issues that we have talked about for years on steroids. Why? I will list a couple of reasons.

Mobile phones are tied to a specific person. Most computers aren't. Because there are more opportunities for tracking, with a mobile device you have someone's location, and it is always with you. And we found out that it is always busy during the night as well for many people today.

The average smartphone owner spends more time on apps than they do talking on it or browsing the web. This is an issue because mobile apps are far less transparent about how they use your data than most websites. Nearly three-quarters don't even have a basic privacy policy, and mobile browsers don't have nearly as many privacy controls as Web browsers do.

In the end, we are all involved in protecting kids' privacy in the online and mobile world. But we can also protect our—but we can't protect our kids' privacy if companies and operators aren't providing real opportunities to do so.

So what do we at Common Sense Media propose? We urge Congress to bolster laws protecting essential privacy for our Nation's children and teens. There are five principles which should be essential elements of any new legislation from Congress.

First of all, number one, the industry standard for all privacy should be opt-in, especially for kids and teens, private by default and public by effort. And today, it is the other way around.

Number two, privacy policies should be clear and transparent. You shouldn't need to hold a degree from Harvard Law School to figure out how to decode a privacy policy.

Three, no behavioral tracking of kids. There are limits on advertising to kids on TV and cable, not on the web. Kids are not little consumers. They are children. Let us not invade their privacy and then pummel them with ads.

Number four, parents and kids should be able to easily delete online information. Too often we hear about young people who post information they later regret and find that they can never fully de-

lete it from the online world. We have to protect these kids from permanent damage.

And finally, number five, we must vastly increase education and information about online privacy. Kids and parents need to do their part to protect privacy and the privacy of their friends. A large-scale, multi-year education campaign would help them learn how to do so effectively. Industry leaders could play an important role in this and should be required to finance it.

Honestly, we wonder why leading tech companies seem to consider privacy implications for children and teens only after the fact. These considerations should be baked into the design phase of a product or service. Companies now successfully do this for disability access. Why can't we do it for kids' privacy?

A founder of a popular social networking company commented last week in a *Washington Post* interview that, and I quote, "We will figure things out as we go along," when asked about special privacy considerations for youth. Come on, we have got to do better than that.

We all need to work together to find solutions in this space, and we need the tech companies to bring their innovation skills to this crucial and shared goal of protecting our Nation's kids.

Thank you.

[The prepared statement of Ms. Shenkan follows:]

PREPARED STATEMENT OF AMY GUGGENHEIM SHENKAN, PRESIDENT AND CHIEF OPERATING OFFICER, COMMON SENSE MEDIA

"Protecting Privacy—Especially for Kids—in a Mobile and Digital World"

Good morning, Mr. Chairman, and members of the Committee, and thank you for this opportunity to discuss the crucial issue of protecting consumer privacy in the mobile marketplace.

Common Sense Media is a non-profit, non-partisan organization dedicated to improving the lives of kids and families by providing the trustworthy information, education, and independent voice they need to thrive in a world of media and technology.

Nearly two million people visit the Common Sense website every month for reviews and parent tips about media content and the digital media world. Tens of millions more access our advice and information through our distribution partnerships with leading companies like Comcast, DIRECTV, Time Warner Cable, Cox Communications, Facebook, Yahoo!, Google, Apple, Disney, Netflix, Best Buy, and more.

Common Sense Media commends the Chairman and the Committee for this timely hearing on consumer privacy. The stakes couldn't be higher for all of us, and especially for our nation's kids.

Today, millions of kids don't just go online, they seem to live their lives online. Children and teens today are growing up in a media environment that provides an ever-present and ever-changing experience in a new digital landscape—an environment that is changing childhood. A recent study by Consumer Reports estimated that 7.5 million kids under age 13 are lying about their age to be on Facebook—and that 5 million of those kids are age 10 and under. There are tens of millions more who are 13 through 17.

And kids don't just access content online, they create it. They don't simply interact with their peers online, but with adults and companies too.

And in contrast to the childhoods we all had, today's children are growing up in public. They post, search, copy, "friend," "un-friend," tweet, create, distribute, and connect through social networks, apps, and other digital services in ways that can be seen by millions around the world and gleaned by companies as well, including—but not limited to—the companies represented here today.

The Internet is a worldwide platform for accessing information and realizing new educational opportunities, possessing resources for both entertainment and learning. Yet, with all of the wondrous things that the Internet brings to children and teens, the interaction that such kids have with digital technology, apps, and services raises significant concerns about kids' privacy.

Overall concern about consumer privacy is clearly growing. In a Common Sense Media/Zogby International poll last fall, 85 percent of parents said they are more concerned about online privacy than they were 5 years ago.

Moreover, privacy is a concern expressed not only by parents—but by kids too. The same poll found that 91 percent of parents (and 81 percent of teens) say search engines and social networking sites should not share their physical location with other companies without their specific authorization.

Yet, lest you think that Common Sense Media is a Luddite organization, let me emphasize that we embrace technological change and innovation and the manifold benefits the Internet and digital media bring to children and teens. One of our founding beliefs is that "we love media." Like the millions of parents and teachers who come to Common Sense for information, we want to find the best things that the digital media world offers for kids—and there are many great things—but also want to avoid the things that may not be appropriate for them, especially at younger ages.

We simply believe that a far better balance can and must be struck. A balance that makes available the rich resources of the Internet—but that also protects children and teens from privacy invasions and inappropriate targeted marketing and behavioral advertising. There is no such balance today, and the basic well-being of our children and teens is at risk as a result.

We believe that balance is being struck in a bipartisan way on the House side by legislation introduced by Rep. Ed Markey (D–MA) and Rep. Joe Barton (R–TX), the first major kids' privacy legislation introduced since 13 years ago—when the founder of Facebook was in grade school.

And as much as we embrace overarching, comprehensive privacy protections for consumers—and especially kids—for all Internet technologies and services, it is clear that the ability to track the mobile whereabouts and habits of an individual as she or he moves throughout our society raises hyper-sensitive privacy issues. Privacy is an issue everywhere in the online world, but in the mobile world, privacy is an issue on steroids. And this Nation must address the issue of mobile privacy now. We cannot overstate the urgency of this moment.

For kids, this is absolutely critical—knowing what a child or teen does online at home is one thing. Knowing where they go after school, with whom they visit, what they search for, and what hours they spend where around town is not only incredibly invasive, it is potentially very dangerous and a fundamental violation of their personal privacy and self-interest. Mobile companies and app developers that have a cavalier attitude about this topic need a very clear wake-up call. While all adults should have "opt-in" protections for location information for all mobile services and apps, it is vitally important to move immediately to protect children and teens in the mobile environment.

Concerns about mobile technology and geolocation have been reinforced in several recent surveys and studies. For example:

- In a survey by TRUSTe, an industry-based organization, 77 percent of smartphone users said that they don't want to share their location with app owners and developers.
- In a recent Nielsen survey of mobile subscribers who downloaded an application within the previous 30 days, more than half (59 percent of women and 52 percent of men) said they are concerned about their privacy when using geolocation services and check-in apps.
- A new study by the Future of Privacy Forum analyzed the top 30 paid mobile apps across the leading operating systems (iOS, Android, & Blackberry) and found that 22 of them -nearly three-quarters—lacked even a basic privacy policy. This is outrageous, especially because kids are such huge users!

It is obvious to most of us and clearly to most parents that our existing protections for privacy and personal information online are grossly inadequate and in no way keeping pace with the rapid changes of our digital and mobile media world.

Congress must address this critical issue for kids and families now. Congress enacted legislation in the late 1990s addressing wireless location information from wireless carriers requiring such companies to obtain the "prior express authorization" of the subscriber for using location information for commercial purposes. But this outdated law did not cover 3rd party services and apps—only wireless companies—and did not contain specific protections for children and teens. That should be changed now.

Moreover, in the case of children, as you know, the Children's Online Privacy Protection Act (COPPA) is the landmark legislation in this area, but the technological advances that have occurred since 1998 make COPPA woefully out of date for keep-

ing children safe from these vast new threats to their privacy. 1998 is like the medieval ages of digital tech development, but that is when the last privacy law protecting kids was written.

Common Sense Media believes it is way past time to update that Act and to provide major new privacy protections for children and teens, on mobile platforms and elsewhere.

If we want to strike the proper balance, and ensure that America's kids and adults can realize the benefits, and avoid the potential pitfalls, of the digital world, all of us—parents, educators, policymakers, and industry leaders—can and must take steps to improve protections for our privacy and personal information online, and especially for kids. But Congress must lead now.

For kids, Common Sense Media believes those steps should build on a few basic principles. The first is Do Not Track Kids. Period. Full Stop.

Children and teens should not have their online behavior tracked or any other personal information about them collected, profiled, or transferred to other parties. The 1998 COPPA categories of "personally identifiable" information (*e.g.,* name and address) must be updated to include other "persistent identifiers" and to encompass all activities in the online and mobile world. What children and teens do online should remain private.

Companies—whether Internet service providers, social networking sites, third party application ("app") providers, data-mining companies, or advertising networks—should not be permitted to collect, store, use, sell, or transfer that information at all. And Congress must pass a law with teeth in order to enforce this prohibition.

Today many companies troll the Internet to collect our kids' detailed information in order to target them with "behavioral marketing"—advertising that is specifically tailored to their age, gender, interests, and activities. Behavioral marketing to kids is unfair and deceptive, and it should stop.

Without parents or kids knowing it, companies collect, store, and sell information about what kids do online and on mobile phones. Companies can install "cookies" or other devices that track which websites kids visit, including which pages they look at; what searches they make; which videos they download; who they "friend" on social networking sites; what they write in e-mails, comments, or instant messages; and more.

And thanks to geolocation services, companies can now also track where kids go in the physical world as well as the virtual one.

Obviously, some online tracking is a helpful aspect of Web 2.0 technology, and parents or teens over the age of 16 should be able to "opt in" to limited use of tracking devices, as long as they are not used for behavioral marketing and are not transferred to third parties. This is the second major element of a legislative effort to protect the privacy interests of kids.

Because of the dramatic growth of mobile technology and geolocation services, it is absolutely essential that privacy protections apply across all online and mobile platforms. And this Committee and the Senate should pass laws to that effect in this Congress.

Many kids today don't merely go online—they always are online, whether from their home computer or from a cell phone, iPod, or Web-connected video game console. To reflect today's mobile and digital world, privacy regulations need to be vastly expanded and applied to all online and mobile services and platforms. Social networking sites shouldn't be able to collect or sell kids' private information, and neither should third-party apps on those sites. Geolocation services shouldn't be allowed without clear prior consent—a formal opt in by a parent—regardless of what type or company or operator provides the service.

It's important to note that just as we say, "we love media," Common Sense also loves mobile technology, including for kids, but we are highly cognizant of the downsides as well, especially where the fundamental privacy rights of children and teens are involved.

In April 2010, we published a white paper "Do Smart Phones = Smart Kids? The Impact of the Mobile Explosion on America's Kids, Families, and Schools."

That paper highlighted the vast expansion of mobile technology usage by kids, and also the ways that smart phones and devices can help kids learn, explore, and engage. But we also highlighted some of the extraordinary potential downsides of mobile media, including ways that these devices may make it easier for kids to engage in inappropriate—and even dangerous—activities. These include cyberbullying, sexting, and distracted driving. Most importantly, Common Sense raised a number of critical questions about the potential downsides of mobile phones and geolocation technology:

Mobile phones with GPS capabilities can expose a kid's exact location. Many new programs and apps have been developed that allow kids to announce their physical whereabouts. This creates physical safety concerns. If a kid shares location info to "friends," that information can be passed along to unintended audiences. Privacy concerns are also a huge issue. Marketers use geo-location technology to target kids with promotions. A child's purchasing habits will be registered and personal data collected. Location-based technology raises several critical questions and concerns:

- Should mobile geolocation data, persistent IP addresses and other identifying information be protected for children under age 13—in the same way that name, age, gender, and address information are protected today?

(*Clearly. And there should be protections for 13 to 17 year olds as well.*)

- Do teens understand how their personally identifying information will be used, and do they need additional protections?

(*Obviously not, so the privacy of teens must be protected by clear legislation.*)

- Will this identifying information be used to target kids and teens with new behavioral advertising and marketing campaigns?

(*Sure, unless Congress forbids this practice, as it should.*)

There are several additional key principles I'd like to highlight briefly from our recent policy brief, "Protecting Our Kids' Privacy in a Digital World"—which should be essential elements of new privacy legislation from Congress this year.

1. The Industry Standard for All Privacy Should Be Opt In—Especially for Kids and Teens

Companies and operators must make significant changes in the ways that they collect and use personal information. The industry standard should always be "opt in"—companies and operators should not collect or use personal information unless users give explicit prior approval.

The opt-in standard is fundamental to our ability to control our personal information. If online companies, services, and applications want to collect and use personal information, they should get permission beforehand by asking people to opt in to the service. And for kids and teens under 16, this means getting their parental permission up front.

Far too many online and mobile companies launch new services—including geolocation-based applications—and enroll users automatically, giving them the opportunity to opt out afterward. This can mean that kids' personal information is collected and used before the kids or their parents even understand how the service works. All online companies, services, and third-party application providers should follow an industry standard of obtaining a clear opt in, especially for kids.

2. Privacy Policies Should Be Clear and Transparent

Privacy policies must be easy for all users to find and understand and should be carefully monitored and enforced. Instead of lengthy legal documents, companies should use icons and symbols that would clearly and simply convey how—and why—users' personal information will be used. We need clear, succinct language for privacy policies, especially for kids.

3. The Eraser Button—Parents and Kids Should Be Able to Easily Delete Online Information

Children and teenagers should have the opportunity to delete any and all information they have provided about themselves. Too often we hear about young people who post information they later regret and find they can never fully delete from the online world. Children and teens post personal information on websites, virtual worlds, social networking sites, and many other platforms. Children also make many mistakes when it comes to their privacy. They should be protected from permanent damage.

Online and mobile companies should be required to develop tools that make it easier for young people—or their parents—to completely opt out and delete this information. Technological innovation in the online industry over the past decade has been truly amazing; the industry should apply that same spirit of innovation to creating tools like "eraser buttons" so that no 15-year-old has to live the rest of his or her life with the consequences of a poor decision about what to post online. Congress should require this, and my talented colleagues on this panel should spend some of their companies' profits to make this a reality.

4. We Must Vastly Increase Education and Information About Online Privacy

Kids and parents need to do their part to protect their online privacy—and the privacy of their friends. A large-scale, multi-year public education campaign will help them learn how to do so effectively. Industry leaders could play a significant role in that campaign, and should be required to finance it.

The online and mobile world is changing so rapidly that children, teachers, and parents all need to be educated about their online privacy rights and needs. Every school in the country should offer a digital literacy and citizenship curriculum, with privacy as an essential component, and this should be funded by industry profits.

Educating and informing consumers is a core element of Common Sense Media's work. We provide parents and families with reviews of media content, so that they can make informed choices and find media that is appropriate for their children. Recognizing the growing use of mobile devices and mobile apps by kids, Common Sense began reviewing mobile apps last year, and our site now features more than 1,000 reviews of apps for kids. In many cases, our editors and reviewers recommend these apps for kids—but when the apps use geolocation technology to broadcast the user's physical location, like "Loopt Mix—Chat!", our reviews make clear that we don't recommend them for kids, or at least not until they are older teens. But today, there are no required app ratings, and not a single mobile company has taken this issue seriously. Congress should require them to change that reality today.

Balancing Opportunities and Potential Pitfalls

At Common Sense, we recognize that mobile devices and geolocation services can create new opportunities—for learning, exploration, communication, and commerce—for kids and adults. Yet they can also bring enormous threats to our privacy and personal well-being. But whether their impact is positive or negative, mobile phones and devices are not going away. As parents, teachers, industry leaders, and policymakers, we must all take steps to ensure that kids can access the benefits of mobile technology and digital media, while protecting them from potential negative consequences.

Whether our first concern is protecting the best interests of kids and teens, or preserving and expanding a marketplace for all consumers so that tech companies can make profits and innovate, we all have a role in building a mobile environment that is trustworthy and safe. The extraordinary technological changes and new mobile and social media platforms that have developed in recent years have created entirely new environments for children and teens, with unprecedented and extraordinary implications for their privacy. It is time to update our Nation's privacy policies for the 21st century. They are terribly out of date. Everyone needs to be a part of this new effort: industry, families, schools, policymakers, and young people themselves. But most of all, this Senate and this Congress need to pass fundamental privacy protections for kids and teens—and their families—now.

Thank you very much.

Senator PRYOR. Thank you very much.

And again, we are going to do 5-minute rounds here on the questions.

I would like to start with you, if I can, Mr. Reed? And I want to ask about the *Wall Street Journal* article. I think you referred to it, or someone did, a few moments ago about the smartphone apps transmitting information.

And we have a little chart that shows some of the companies. I think maybe it is the—if I am not mistaken, it is their top 12 or something like that, that they listed in the article.

And Mr. Reed, how do you propose notifying consumers in a better, more meaningful way so that they are not surprised to learn that their information is being sent to folks or that they are being tracked?

Mr. REED. Well—oh, sorry—first of all, I think it is a great thing to look at in terms of informing the consumer. One of the best things about the *Wall Street Journal* articles is that they help do an education job that we in the industry—remember, most of my members are 3, 10 people—have had a hard time doing it ourselves.

So we benefited from that right off the front end. We were able to tell consumers, "Hey, this is part of what we are doing, and the privacy policies that we have in place are there."

Now we face two problems as an industry that have been talked about a lot. The 2-inch screen problem—how do I write a privacy policy that holds up to fine lawyers, like yourselves and others, that is simple and easy to understand and can be displayed in a 2-inch screen? So that is one hurdle that we as an industry are facing.

My members want to deliver the clearest, simplest privacy policy. But when they go to a lawyer to have it checked, many come back and say, "Well, you need this proviso."

The second part of this has to do with the constantly changing world that we face in terms of business models. We started out this whole apps world only 3 years ago. At the time, we had an app store at Apple, which you sold directly, you got paid for. We didn't have advertising at all. Recently, we added in-app purchasing.

So having a private policy that not only reflects the business model today, but encompasses the business model tomorrow, the changes that Apple can make at any time to their privacy policy—or that Facebook can make or that Google can make—are all part of the problems we are having in trying to address it.

So what we have done with our working group is we have not only brought in regular developers who use ads, but we have been focusing on developers who actually do multiple business models. And we have brought in ACT member Privo, which is one of the four recognized FTC safe harbors for COPPA, to help us create guidelines that can actually address the important questions that were raised earlier about children.

Senator PRYOR. OK, great. I think that we need to follow up on that a little bit more.

But first, Mr. Davidson, let me ask you. You talked about when you opened your Android phone and that screen came up, and if you wanted to, you could check "no" for the tracking for the—what do you call it—geolocation?

Mr. DAVIDSON. Right. Our location services, yes.

Senator PRYOR. And that's great. But what happens if then you start using the phone and you start adding apps that do require that geolocation? What happens then?

Mr. DAVIDSON. It is a great question, and I think it is a very important question. So the way we have addressed that is when you try to install an application that wants to use location services—Foursquare or something, you know—you get a notice before the application is installed that says, "This application wants to use your location information. Is that OK?"

And you actually have to accept that before installing the application, so—and we give notice about other kinds of information that the application might want. We do it very simply. It is usually not more than a screen. Maybe sometimes you have to scroll down a little bit, but it is not a multi-screen thing. We have worked very hard to make it very simple. And the key is—this is, I think, what we were talking about at the last panel—timely notice and a choice for consumers.

Senator PRYOR. OK.

Ms. Shenkan, let me ask you—you mentioned your five principles that you like. When I hear Mr. Davidson talk and others talk, I also know that there are, you know, very legitimate reasons why parents may want to track their own children. You know, they may want to know where they are. Would your five principles allow parents to do that?

Ms. SHENKAN. That is a good question. We haven't contemplated it. I guess the best answer probably is we should get back to you on that. Of course, it would depend on the age of the child.

Senator PRYOR. Right. Well, as a parent of two teenagers——

[Laughter.]

Senator PRYOR.—let me say that there is a parental interest in this.

[Laughter.]

Senator PRYOR. You know, it just—it could be a good thing, depending on the family. But anyway, yes, I hope you will think about that as you go through. Because when I heard your five that you laid out, they seem kind of ironclad, and I am not sure you had enough leeway in what you were doing to think about that. But anyway, if you could consider that, I would appreciate it.

Ms. SHENKAN. Yes. Yes, thank you.

Senator PRYOR. And let me ask you, Ms. Novelli, before I turn it over to other colleagues on the Committee here, you talk about your privacy policy. All that sounds great. But can you tell—can Apple tell how many people actually read it?

Ms. NOVELLI. Well, they have to say that they agree.

Senator PRYOR. Right.

Ms. NOVELLI. We can't know for sure if they have read it. We try to make it in plain English and very short, but we can't tell if you have—we can't watch someone reading it.

Senator PRYOR. Well, but can you tell how long they are on those screens? Do you have any way of knowing that?

Ms. NOVELLI. I don't know whether we can or can't, sir, so I will have to get back to you on that.

Senator PRYOR. Just my guess is, for a lot of folks, it is just too much information, and they just kind of agree without really understanding what they are agreeing to. But that is another matter that we can discuss.

Senator Rockefeller?

Senator ROCKEFELLER. Thank you, Mr. Chairman.

Bret Taylor, this would be to you. Under Facebook's terms and conditions, a user must be 13 or older to have an account on your website. Despite this, according to a recent *Consumer's Report* study, an estimated 7.5 million users were younger than 13. Moreover, the Facebook app in the Apple App Store is rated for age 4 and above.

Now my question to you is, I understand it is Facebook's policy not to allow children under 13 to have an account. But the description of the Facebook app and the Apple store rates the app as appropriate for age 4 and older. How is that consistent with your policies, and who determines the rating for Facebook's app?

Mr. TAYLOR. Senator, thank you.

That is a very good question and actually news to me. So my—first of all, we don't allow people to have accounts under the age

of 13. If I had to guess, my guess is that because the Facebook application doesn't, in and of itself, contain mature content, that is what the rating reflects. But I think we can follow up with your office about why that rating exists.

And certainly, our iPhone application has the same rules and conditions governing it as our website, which means that no one under the age of 13 can create an account.

Senator ROCKEFELLER. And I appreciate that. But it doesn't appear to be the truth. You have 7.5 million under 13. This takes me back—and I won't harp on it. But Facebook grew so fast. Zuckerberg gets that in Harvard. He is 20, 21 years old. He comes up with a big new idea.

It is my general feeling that people who are 20, 21, 22 years old really don't have any social values at this point. In his case, I think he was probably——

[Laughter.]

Senator ROCKEFELLER. No, I am serious. I think he was focused on how the business model would work. He wanted to make it bigger and faster and better than anybody else ever had. And nothing I know suggests otherwise.

So that you can't just dismiss that 7.5 million users are younger than 13 and say that you have a policy that doesn't allow that to happen. I asked Sheryl Sandberg. I am very worried about suicides, people stalking youngsters. They innocently put themselves on a blog and think it is just going to one person, and it goes to Indonesia and everywhere else, and you have 600 million people.

And I asked her who signed up. And I asked her, well, how many employees does Facebook itself have? Now this was 2 or 3 months ago. She said 1,600 worldwide. I assume she is right. She is number two in the company. So I assume she was right.

And then I said, well, how many people do you have monitoring the box to see what is being said because I am, as are you, worried about what can happen to children—humiliation, bullying, predators, all the rest of it. I think it is a huge subject.

And I have town meetings all over West Virginia on this subject, not necessarily on Facebook, but just in general. Parents are terrified. They are terrified. And they don't know what to do. School counselors don't know how to handle it. You get a whole group in, and they are very worried about this.

And she said we have 100 people who monitor these 600 million people, who, I assume, are doing a whole lot of blogging every day. And my reaction to that is that is just absolutely indefensible. It is unbelievable that you would say that.

And she said, "we are going to do better in the future." And I want you to defend your company here because I don't know how you can.

Mr. TAYLOR. Well, Senator, I just want to say we really emphatically agree with your points. And I just want to clarify a couple of issues.

First, whenever we find out that someone has misrepresented their age on Facebook, we shut down their account. I am not sure of the methodology of the study you refer to, but I can tell you emphatically that we don't allow people to misrepresent their age. And there is a couple of interesting points here.

Senator ROCKEFELLER. But when you say we don't allow people to misrepresent their age——

Mr. TAYLOR. Yes.

Senator ROCKEFELLER.—you don't, and you can't. How can you do that?

Mr. TAYLOR. Well, Senator, it is a very good question and something we have thought a lot about. What we have found is the most scalable way, both in terms of age enforcement, but also the other issues you brought up around bullying and other protections of minors on the site are baked into a system of enabling people to report problems on the site.

I will talk about bullying first, because I think it is an important issue you brought up, and then talk about age protection. We have—under almost every single piece of content on the site, we have a link where individual users of the site can report inappropriate content and report bullying. And originally, that would go into a special queue that our user support department would take and bring down the content almost immediately.

We have also expanded that, though, with a program we call Social Reporting that enable people not only to report it to us, but actually report it to parental and teacher authority figures who are also on Facebook. So if you are a minor on the site in high school, and you see an inappropriate picture, as I think was brought up in one of the open meeting testimonies, you can not only report to Facebook and have it removed, you can report it to a parent or a teacher who can actually deal with the underlying cause of why someone would post a picture like that and actually deal with it offline and deal with the underlying issues.

We obviously—we actually have about 250 people working across safety, privacy, and security at Facebook. But in addition to that, we have mixed those with these self-reporting mechanisms because we find they are very accurate.

Regarding age, that is——

Senator ROCKEFELLER. You know what? My time is up, and I want to get a comment from Ms. Shenkan.

Mr. TAYLOR. Thank you, Senator.

Senator ROCKEFELLER. Thank you. I apologize to you.

Mr. TAYLOR. No problem.

Ms. SHENKAN. On the same question?

Senator ROCKEFELLER. Correct.

Ms. SHENKAN. You know, our view is, again, that not enough is being done. If we took a small amount of the time that any of these companies spend innovating products and started to think about how we protect our kids—and frankly, adults, but we are focused on kids—we think that would go a long way.

I mean, these are the organizations that have created a platform which 600 million people across the globe use, companies that have mapped every street in America so that we can all—across the world so that we can all use. And instead of spending money to try and hire PR firms to try and take down the other company, let us take that money and spend it on figuring out technological ways that will protect our kids. It can't be a hundred people sitting in a Facebook office, trying to monitor 600 million conversations.

Senator ROCKEFELLER. Thank you.

And thank you, Mr. Chairman.

Senator PRYOR. Thank you.

Senator Klobuchar?

Senator KLOBUCHAR. Thank you very much, Mr. Chairman.

We have been talking some about how we get privacy policies that are understandable and readable and yet a lawyer will draft. And I know that, Mr. Davidson, when you were asked at the Judiciary Committee about this, you were asked whether you would commit to requiring apps in your store have a clear, understandable privacy policy. And you said you would take the question back to your leadership.

Have you heard anything back on that, and will Google commit to requiring apps in your app store to have a clear, understandable privacy policy?

Mr. DAVIDSON. We think that apps should have a clear, understandable privacy policy. I do not have an answer for you today about whether we will make it a requirement in our app store. We try to make our app store as open as possible for all the small businesses who use it.

I think those apps should have a privacy policy, and we are going to work to try to figure out how to enforce it. We do enforce things like COPPA on our app store.

Senator KLOBUCHAR. OK, thank you.

And then, Ms. Novelli, you were asked by Senator Coburn—I am on Judiciary as well, so I was looking back at the transcripts—in a judiciary hearing, the one you had last week, that you were asked about testing apps. And you were saying how Apple tested an app and did random spot checks. So, presumably, you might spot any problems.

And yet, *The Wall Street Journal* found that there were problems with some of the apps in terms of sharing location data without informing the user. How do those two things mesh?

Ms. NOVELLI. Well, we do our best to check for all of our requirements that are in our developer agreement. We do randomly audit. One of the requirements that we have is that you must get permission from the—to share information.

With respect to location, there is a requirement that if you want to use the location data of a consumer, you have to pop up a dialogue box that is linked into our API that we designed that says we would like to use your location, allow or don't allow. And I can't comment on specific apps, but I believe that was not the particular question that was referred to.

But when we find a problem or someone alerts us to it, we immediately investigate and work with the developer. They have 24 hours to fix the problem or be removed from the store. What we have found is that developers have a great incentive to fix the problem.

Senator KLOBUCHAR. OK.

And Mr. Reed, you have been working in the area of trying to put together a comprehensive set of guidelines for app developers that will follow clear policies, and I support that effort. I think it is good.

But I look back and think that considering anyone with skills and a computer can build an app, do you believe that a self-regu-

latory approach to privacy will be enough to keep the bad actors out of the market?

Mr. REED. Well, I think there are two parts. I think that the self-regulatory approach is the way we have to start, but I don't think it is truly self-regulatory. We heard earlier from the FTC. We think the FTC has and should strongly enforce Section V.

And in fact, I know that—in this case, I won't speak from the legal side of it, but we see deceptive and unfair should include or conceptually should include someone who misuses your data and just doesn't have a privacy policy. I know that we heard earlier that the FTC is unsure about that. But I see no reason why if someone is misusing your data that doesn't fall into the realm of an unfair and deceptive trade practice.

So I would say we want to start with self-regulatory. We want to bolster our industry's effort on that. And the second side of the—the stick side of that would be the FTC coming after folks who misuse data and don't have a privacy policy.

Senator KLOBUCHAR. OK. And then, Mr. Taylor, I know Senator Rockefeller was asking you about the number of kids who might be claiming they are 13. For kids, I don't know, under 18, do you see a different way of trying to reach out to them to talk about the privacy policies? And are you thinking about that in terms of making sure that they understand it that you might use a different approach than with an adult?

Mr. TAYLOR. Yes, it is a really good question and something we have thought a lot about. Fundamentally, we agree. I think most people in this room agree that minors, people under the age of 18, should have a different experience on Facebook because of the unique needs and privacy protections and security protections that a minor needs, and that makes its way into all aspects of our product, not just a legal privacy policy.

So on Facebook, if you are a minor, you actually have a different experience. Your privacy setting defaults are different. When you share things, it goes to a more restricted audience.

When you report problems on the site, our user operations respond differently if it is a minor. And it really makes its way throughout our product. And that applies especially to privacy and security issues.

Senator KLOBUCHAR. OK. Thank you.

And then, Ms. Shenkan, last follow up with some of Senator McCaskill's point, not all data sharing is bad. And in fact, much of it can be beneficial to both the consumer and third parties.

So the question is where you draw that line. And more targeted advertisements can be more relevant and helpful to the users. However, as you know, there is this line between sharing data and tracking. And where do you see the line, and what common practices do you think cross it?

Ms. SHENKAN. Thank you for the question, Senator.

If behavioral targeting or advertising is so useful to consumers, they have should have the ability to say "opt-in." So if I happen to be on Facebook and I am writing to a friend or posting on my wall about wanting to go see Elvis Costello, and I say, you know, that it is fine to track and monitor my conversations and advertise to me on that, and I get an ad, then that was my choice. And I obvi-

ously saw the value of providing my information to get something back.

Also I think that—just if I can—I thought that Senator Kerry made a really fundamental point in his statement when he said that he rejected the notion that there is a choice, fundamental choice that needs to be made between innovation and protecting privacy. We couldn't agree more. That is a false choice.

The entire—the Internet economy in the U.S. alone will be close to $200 billion in e-commerce. Most of that was not created by harvesting private data and using it to behavioral target people.

In fact, one of the beautiful things about search engine advertising is that customers are opting in every time they go onto a search engine. They are putting up their hand, and they are saying, "I am in market for a new car or truck, so please advertise to me."

And that is OK, and it can work that way. And $15 billion a year are spent by advertisers in that part of the economy, and that is fantastic. And that is an example of where privacy is protected and innovation has happened.

Senator KLOBUCHAR. OK. Well, if any of you all want to respond, I think I am out of time, but we can talk about it later.

Ms. SHENKAN. Thank you.

Senator KLOBUCHAR. OK. Thank you.

Senator PRYOR. Thank you.

Senator Blunt?

Senator BLUNT. Thank you, Chairman.

Mr. TAYLOR AND MR. Davidson, I am going to ask you in a minute if there is any example you have of a problem that the company self-corrected. You know, one of the things I hear is when there are problems that usually the company moves forward and self-corrects them before anybody else even knows they are a problem. And a couple of examples of that would be helpful, if you have them.

Ms. Novelli, do you—does Apple track the location of my iPhone?

Ms. NOVELLI. No, sir. We do not track the location of your iPhone——

Senator BLUNT. Don't track the location?

Ms. NOVELLI. We do not, sir.

Senator BLUNT. And is it—are you—is it logging in right now? It is on. Is it logging in, or are you—is there some log-in system that you look at for my iPhone?

Ms. NOVELLI. No, sir. Apple does not look at a log-in system for your iPhone.

Senator BLUNT. So what do you do? How does it work that I might get some advertisement for something?

Ms. NOVELLI. An advertisement on an app?

Senator BLUNT. I will be solicited on an—well, on an app or through my mail account or whatever.

Ms. NOVELLI. Well, sir, there are no advertisements on the mail account that is on your iPhone. You could get an advertisement. There is a Web browser on your iPhone that is just like if you used your computer, our Safari Web browser. And that works the same as it would as if you were working from a computer. So that if you are logged onto a website——

Senator BLUNT. But I would have to be doing—on something for that happen you are telling me?

Ms. NOVELLI. Correct. That is correct, sir.

Senator BLUNT. What is crowd-sourced—what is a crowd-sourced database?

Ms. NOVELLI. That is a—essentially what it is, sir, is a map of the locations, the geolocations of cell towers and Wi-Fi hotspots that we derive from information that is anonymously sent to us from people's phones, from iPhones. So the phone, when it goes by a location, will send saying, "There is a Wi-Fi hotspot here. There is a cell tower there." There is nothing that connects it to an individual or the individual's phone.

And we are using that map to help people later on when they want to know where they are. And it is a simple process of being able to know where you are relative to fixed points, just like a regular map works.

Senator BLUNT. OK. Mr. Davidson, back to my other question. Did you think of an example of something that could have been a problem that you all just went in and self-corrected?

Mr. DAVIDSON. I think we are constantly innovating. I don't know if it is always about fixing problems. But I will give you a couple of examples. We take the comments from Ms. Shenkan very much to heart about trying to do more to protect children.

So, for example, relative recently, we just launched a PIN lockout feature on Android so that parents could control—could make sure that—or anybody could make sure that their phone isn't downloading apps without a PIN. We have expanded our Safe Search program, which is a project to enable people to set controls on search results to make sure that they are child friendly.

We have just added a flagging mechanism in Android so people can flag bad apps. This is similar to what Mr. Taylor was talking about. These are all things we have done. I think they have all been improved in the last 6 months.

Now I would say, you know, some of them are really about trying to make sure that we are doing more and always doing better to protect children. There have probably been other things that we have done that we are constantly trying to correct.

Senator BLUNT. Mr. Taylor?

Mr. TAYLOR. Yes. It is a very good question, and I think, to Mr. Davidson's point, in the industry we are constantly working to improve the security and safety of our products because it is the basis by which people choose to use them. And if they lose trust in a service like Facebook, they will stop using it.

I think a very timely example is actually this Friday, we will be announcing, in partnership with Microsoft and the National Center for Missing & Exploited Children, we are going to be deploying a photo technology that Microsoft Research developed to identify, using relatively sophisticated fingerprinting technology, pictures of missing and exploited children, both to prevent child exploitation on Facebook and help people find missing children.

And that is something we did proactively and in partnership with these two organizations because we care deeply about all these problems, just as all of you do.

Senator BLUNT. Ms. Shenkan, you mentioned something. I just want a little clarification. We need to protect kids from permanent damage. I assume that meant if they had put something out there for people to see.

How do you do that if people have already seen it and somebody has already captured that? Assuming that kids have access to this way to communicate, how do you protect them from permanent damage if they have made a decision to put something out there that is damaging?

Ms. SHENKAN. The issue—thank you for the question.

The issue is that the information is not only public when somebody puts it up, which is hard to control, but it is that it is persistent. It is very hard to take the information down. We have talked about in one of our privacy briefings the concept of an eraser button, where it would be very easy for somebody who realized that they put up something that they didn't want up there, that they could then take it down.

Senator BLUNT. But once you put it up there, can't somebody else capture it, and then they have it?

Ms. SHENKAN. Yes, and that is the problem. I mean, again, you know——

Senator BLUNT. But I mean, that is the problem of putting it up there is somebody else can capture it. And then they have it, and they can share it. Is that—am I wrong on this?

Ms. SHENKAN. Yes—no, that is the problem.

Senator BLUNT. Yes. I don't know how you—how you stop permanent damage if somebody does something that is damaging, unless it just happens that nobody sees it and nobody else decides they want to use it. The problem here is access.

It is very scary. Any of us who have children or grandchildren, it is very scary to think of what somebody might do. But I am not sure we can actually ever come up with a fence that is high enough or big enough to stop that from happening. And you know, it does have that terrifying long-term problem. But if people have access and they put information out there, it is out there.

Ms. SHENKAN. Yes. Well, and there is an industry blossoming that you can pay companies to go spend time every month taking down information that is posted about you online. So people are figuring out ways to do it.

What we would like to see happen is the companies in this room and elsewhere figure out how to make that much, much easier.

Senator BLUNT. Mr. Davidson? Then my time is up.

Mr. DAVIDSON. I would just add, and I know this isn't the most attractive solution, but a huge part of this is about education. And I have young children. I would just say I think—you know, there is a recent report from the National Academy talked about some of these problems and said, you know, you could try to build a fence around every swimming pool, or you can teach children how to swim.

And I think what we really need to work on is how to teach children how to be literate in this new world. And that is a very, very big project.

Senator BLUNT. Thank you, Chairman. I am sorry I went over.

Senator PRYOR. Thank you.

Senator McCaskill?

Senator MCCASKILL. Thank you.

I got a Tweet from my last round of questions I want to address. I didn't mean to sound flippant about HIPAA. I don't know if "AM Privacy" is in the room. But if you are, what I was trying to say about HIPAA was that the bottom line is that we had some unintended consequences and some costs that came with HIPAA.

That 2-inch screen you talked about? We clearly didn't get that down on HIPAA because most people who are going to the doctor's office are not reading the long thing that they have to read, and they sign. And I bet most people in this room would admit if they go to the doctor, they are not reading the whole long thing they sign on HIPAA, and you have to sign one or two or three of them every time you go, which adds administrative costs in.

And there were some unintended consequences in terms of finding people that might have similar very—some of the diseases that are very unique and rare, trying to find people for research purposes. HIPAA has stood in the way of some things that were a problem.

That doesn't mean we shouldn't work on privacy. I am just being cautionary that we want to be very careful as we move forward on privacy because so much of the success we have had in this space in our country in the Internet and in the advance of technology has been remarkable. And I want to make sure that we don't have unintended consequences. So whoever "AM Privacy" is, I am glad that I could clear that up before I ask my questions.

I want to make sure that everybody understands how easy this is in terms of turning off things. I mean, not only do I have the ability to make sure that I don't have any location services on here. I can even go down, and you tell me every single app that is using location services, and I can individually go to each one and turn each one off.

The other thing that you do is that you tell me if anybody has used my location in the last 24 hours. There is a little logo that pops up, and so I tried it while the others were questioning. I went on Kayak, checked out a flight, and now there is a little arrow there that tells me Kayak used my current location as I was looking for flight.

Now all I have got to do is just flip that switch, and Kayak—I am telling Kayak it is none of their business where I am. Very simple, very easy to find, right on the page.

So now, here is the thing I wanted to ask Ms. Novelli and Mr. Reed. I am a little confused why "Cut the Rope" is on that list. I am a little confused why "Paper Toss" is on the list.

And it seems to me if we are talking about just games—I mean, "Paper Toss" is a game where you try to get a—it was one of the ones listed in the *Wall Street Journal* article. All you do—there is nothing in that app that has anything to do with location, other than the fact that you are trying to get a piece of paper into a trash can. And it is just a game. Same thing with "Cut the Rope."

So it seems to me if it is very obvious by the app that there is no need for any location, that that could be where the industry could focus on making sure that people understood the consequences. Clearly, the only reason "Cut the Rope" or "Toss the

Paper" is tracking my location is to try to sell to other people where I am going and what I am doing because there is no applicability to the game that is involved.

So it seems to me if you could focus there first, in terms of making sure privacy is very obvious. And when I go on "Cut the Rope" site, which I just tried, and "Toss the Paper," I don't see anything on there that tells me anything about what they are doing as it related to tracking me. So could Ms. Novelli and Mr. Reed respond to that?

Mr. REED. Well, first things first. You raised a good question, and I would say that I often on games like that, I say "no." When it asks me, "Can I share your location?" I just turn it off.

The reality is, is that for some of us who are building applications that are ad-driven, the third-party ad networks will ask us for information so that they can provide a higher-quality ad. One of the things—and then that location information is part of it.

It is interesting to see that there are actually some interesting kind of small-town benefits that we have seen. I will use "Red Laser" because it is a slightly different one. I can hit a—I can hit a SKU. It will tell me the product. It will show me the Amazon price. But right below that, it will tell me Tom's hardware store has that same product. It is $3 more, but guess what? It is right across the street.

Now Tom didn't have to buy an ad from a major supplier. He could actually target it just to that zip code. So there are some benefits to that kind of ad marketing.

But I would also say that you illustrated the first point most readily, which is you want to use "Paper Toss," and you don't want to use the—and you don't want to see the ads that are targeted, turn off location-based services. And I think that is something that we, as an industry, understand and expect some consumers to do.

We have to figure out how we still make money—make money from the ad networks because they control our—they control our income from that. And so, we have to find an agreement with them, rather than us as the tail wagging the dog, where they agree to the terms that you have suggested.

Senator MCCASKILL. Couldn't—Ms. Novelli, couldn't you all—and I know Apple is loathe to do anything to stop the amazing flow of applications that are making your products so desirable, and I get that. But it seems to me on some of these apps that if I had a choice, you can either get it for free and see some ads, or you can pay $2.99 and be ad free and track free.

I mean, it seems to me that is a simple consumer choice that could get—that the industry could do, both Google and Apple, if the two of you did it, and Facebook, to the extent that it would apply to you.

But I think that would go a long way toward consumers beginning to understand, first of all, that when they are being tracked, it helps pay for things, and that is why they get so much free. And it would begin to drive home, there is nothing better than driving home the point of what they are getting for free and how than to give them that simple choice.

Has there been discussion about that? And why haven't you moved toward that kind of model?

Ms. NOVELLI. Well, first of all, Senator McCaskill, there are apps on the App Store—and my husband, in fact, has downloaded a couple of them—where you have that choice. Either it is free and you have to submit to advertising, or you have to pay. And so, there are apps on the App Store like that now.

In terms of the pricing, though, we have the developers set the pricing. We have not really gotten into trying to set prices of apps.

Senator MCCASKILL. No, I don't want you to. I just want you to maybe say——

Ms. NOVELLI. Right.

Senator MCCASKILL.—that people should have the choice as to whether or not they want to pay or whether they want to—they want the ads.

Ms. NOVELLI. And developers have been making that choice, and there are those choices on the App Store now. And I don't know if Mr. Reed wants to comment?

Mr. REED. If I could indulge for 1 second, what you described is exactly what we are doing. And we appreciate that Apple and now Amazon and Google and others are doing in-app purchasing. But remember that that is exactly the model we are using. We are saying on the store right now I have an app in the "Paid For", and then I have one that says "Free" next to it or "Lite." You make a choice which one you want.

Here is an interesting number, though. And we may even subdivide it and say we will do in-app purchases, so you can turn off ads after you have bought the free version.

Senator MCCASKILL. I know, I know.

Mr. REED. Yes, so——

Senator MCCASKILL. And I get—and I don't want to cut you off, but my time is over.

Mr. REED. Sorry.

Senator MCCASKILL. But the bottom line is it is not clear. I get "Lite," I get "Free," and I get "Paid," but I don't really understand when I am making that decision that it also might involve tracking. And that is what I am saying.

I think that might be something you all could do as an industry that might forestall some unintended consequences by aggressive government regulations.

Mr. REED. Thank you.

Senator MCCASKILL [presiding]. Thank you all very much.

And the next questioner would be—it says Senator Udall.

STATEMENT OF HON. TOM UDALL,
U.S. SENATOR FROM NEW MEXICO

Senator UDALL. Thank you, Claire.

Senator MCCASKILL. I am following the list I was given by the Chairman.

Senator UDALL. No, no, no, that is great. Thank you very much.

And I know the Chairman isn't here, but I really appreciate him holding this hearing and all of you responding to the questions of the panel.

As you can see by the questions, there is no doubt that there is a lot of concern in terms of privacy, in terms of protecting minors and those kinds of things. And I really look forward to your supple-

mental answers that some of you are going to give because I think those are some of the key questions that are out there.

And I think from this subcommittee's perspective, we are going to continue to ask these questions and continue to do oversight. And so, I think you should expect that.

Recently, I joined Senators Reid and Schumer and Lautenberg in asking Research in Motion, RIMM; Google; and Apple to stop selling dangerous apps that enable drunk drivers to evade law enforcement. In 2009, drunk drivers killed nearly 10,000 people nationwide, including 141 in New Mexico.

Apps like DUI Dodger, Buzzed, Checkpointer, and Phantom Alert provide drunk drivers with the precise location of DWI checkpoints as they drive. This is in while they are driving around. Some apps even offer audio alerts warning drunk drivers as they approach police checkpoints.

While I agree that public notification of checkpoints on the news or in the paper can serve as a deterrent to prevent individuals from making the decision to drive drunk, providing real-time accessibility tailored to a driver's location only serves to provide drunk drivers with the tools to more effectively break the law and endanger others at a time when their decisionmaking capabilities are already impaired.

And I am very pleased that RIMM did the right thing and immediately pulled these apps from the BlackBerry app store. Why are Apple and Google still selling DWI apps that encourage breaking the law?

And that question, I think, would be directed most to Ms. Novelli and Mr. Davidson.

Ms. NOVELLI. Well, Senator, when we received your letter, the first thing we did is start to look into this and tried to research the whole situation because Apple abhors drunk driving and doesn't want to, in any way, be encouraging it.

What we found when we looked into it is that there were some differences of opinion among reasonable people about whether publicizing, as you note, checkpoints deters or helps drunk driving and that, in fact, some of the information is actually made public by the police forces themselves and is on the Internet.

We are continuing to look at this issue. We will continue to talk with you and your staff as we continue to evaluate it. We do not want to be enabling or supporting drunk driving in any way.

Mr. DAVIDSON. I guess I would echo that sentiment. We certainly appreciate the seriousness of the issue that has been raised. We do remove applications from the Android marketplace that violate our content policies.

But apps that—after an initial review, apps—we determined that apps that merely share information of this sort don't violate those policies at this time. And so, we are evaluating this. We have been talking to your staff. We have appreciated the chance to continue to do that, and we are taking a very serious look at it.

Senator UDALL. Now, as far as Apple's stated policy, you don't—you have a policy that you don't encourage with your apps people to break the law. Is that correct?

Ms. NOVELLI. Yes, sir.

Senator UDALL. And isn't exactly what is happening here is—I mean, you can imagine. You have had our letter now for 2 months.

And you can imagine a person that is drunk—DUI, DWI—driving down the road and they have this—one of these apps turned on, and it issues an alert, tells them there is a checkpoint ahead. Then they can use their device to then find a way around the checkpoint. It seems to me that kind of application is encouraging breaking the law.

Ms. NOVELLI. Well, we are reviewing, as I said, sir———

Senator Udall: Well, you have had 2 months. How long are you going to review it?

Ms. NOVELLI. Well, we will be working with you on this. We are reviewing it. There are some of the apps, for example, that have—a cab number for you to call a cab, alert you that there are, you know, there are checkpoints, and here is a phone number for you to call a taxi.

So I think they are not ubiquitous, all of these apps. And as I said, some of the information is made public by the police themselves. So I think reasonable people have different points of view about how to go about this, and we are trying to do this in the most thoughtful and responsible manner.

Senator UDALL. No, and I understand that. But I hope that you all understand the difference between the police department, the state police, county police, sheriffs, whatever, issuing a broad, general thing that, on Friday night, we are—or Saturday night, we are going to have a checkpoint out there at various points in town.

That serves a deterrent, I think, for people to know. Even though, you know, there is a 2 percent chance of catching drunk drivers. So all of us that are out on the highways, 2 percent chance of catching, you utilizing—somebody utilizing these apps, it makes it even less likely. You know, may drop to 1 percent or half a percent or whatever it is.

But the important point is, is that here you have law enforcement issuing generalized bulletins. But what people do with your apps, and what they are able to do is specifically, in real time, determine there is a checkpoint and evade the checkpoint and possibly afterwards get in an accident and have somebody killed.

So I understand that you all are looking at it closely. But I think this is a crucial question for law enforcement. I mean, I have heard from local police department in Las Cruces. The attorneys general of New Mexico, Delaware, and Maryland have also signed onto this issue and are asking the same questions. And I think the more that this is out there, you are going to be getting these kind of questions.

I am sorry, Mr. Chairman, for running over. But I very much appreciate—I said earlier, your effort at consumer protection and what you are doing in this area is greatly appreciated.

Thank you. Thank you, and thanks to the witnesses being here today.

Senator PRYOR [presiding]. Senator Udall, you are asking important questions. Thank you.

Senator Rubio?

STATEMENT OF HON. MARCO RUBIO,
U.S. SENATOR FROM FLORIDA

Senator RUBIO. Thank you, Mr. Chairman.

Thank you guys for being a part of this. This is very timely and interesting.

Just to close the loop on the Apple portion of it, as an Apple user with a lot of Apple users in our family, I think one of the things that created all this frenzy—and I know the answers to this, but I wanted other people to hear it as well—is the two researchers that found that file on the iPhone and the iPad that appeared to contain the time-stamped record, and then they were able to go out and create an app that basically created that map, the whole thing that flared up in late April.

And the company, I think, acknowledged that that was a glitch and has offered some updates to fix that. Are those updates available already?

Ms. NOVELLI. Yes, sir. Those updates have already been implemented for most of all of the questions. There was one question about encryption that is going to be implemented shortly.

But I would say that, again, that there was no actual information on your phone about your actual location at any time. What was on your phone was essentially like a city map of Wi-Fi hotspots and data bases, not where you were on that map.

Senator RUBIO. Right. But the key to it was that the company's position was that it wasn't intentional. It wasn't our design. It is a glitch that exists.

For example, even if you had—even if the toggle switch had said no, it still was feeding the information, and it was storing it for longer periods of time.

Ms. NOVELLI. Correct.

Senator RUBIO. So the company is now providing a single update, or is it multiple updates?

Ms. NOVELLI. That update went out a couple of weeks ago, and it—there is no more——

Senator RUBIO. Well, but——

Ms. NOVELLI. Which is working perfectly now, and it is not backed up. Your information is not backed up to a computer, and the encryption question is being addressed in our next update.

Senator RUBIO. So someone who has an iPhone or an iPad, that update is available. They still have to pull the update into their device?

Ms. NOVELLI. Yes. It is a free update.

Senator RUBIO. And what would they—just for people watching this—need to functionally do?

Ms. NOVELLI. When they synch their phone, they will get a notice saying there is an update available. Do you want to install it? You say yes, and it just installs on your phone.

Senator RUBIO. So, basically, anyone out there who hasn't updated their phone in the last——

Ms. NOVELLI. In the last 2 weeks.

Senator RUBIO.—should go and update their phones so that this information is all available for them.

Ms. NOVELLI. Yes.

Senator RUBIO. OK. The second question has to do with the relationship with third parties. There is some confusion about that because people go to the Apple App Store or the Android market or Facebook, wherever. When someone buys an application from an online store like that, both from the reality and from the legality perspective, who do they have that—who is their relationship with, their business relationship when they do that?

Like if I go on and I get an application for my phone—and I think this question is for all of you, because I think Facebook does that as well—who do I, at that point, have the relationship with? Is it with you, the marketplace? Or is it the actual app vendor?

Ms. NOVELLI. Well, just from our perspective, once you buy the app and you use it, your relationship is with the app developer at that point. The first-party relationship is with the app developer.

Mr. DAVIDSON. We would agree with that, and usually, for example, a lot of applications, there will be a terms of service you have to agree to when you first install it or something like that. And there is an agreement there.

I think it is why users need to be careful about what applications they use and be thinking about that. It is also why we have tried to give people in our Android marketplace at least as much information as we can before you install the app because that is sort of when we lose the relationship.

Senator RUBIO. I think that point is critically important because a lot of people aren't clear about that. And I know that anyone who sells an app goes through a general screening process. But ultimately, your business relationship is only as good as the company or whoever it is you are interacting that app with. And so, that is important.

Here is my secondary question. If I have a problem with an app—let's say I pull an app into my device, and then, all of a sudden, I start having problems with them, any of these other issues that we are talking about. Let's say I am able to deduce that there is a problem or I get suspicious. Is there a process in place where I can report them to you? What is that process?

Mr. DAVIDSON. So, in our case, we have installed a flagging mechanism so that users can flag applications for a variety of different reasons. And there, you get a check—once you do it, you get a whole set of reasons why you might want to be flagging it, and that is going to a place for review. And that is the starting point for us.

Senator RUBIO. Is that the same for Apple?

Ms. NOVELLI. We have an ability on our app store to contact us. And you can flag any concerns you have, and we investigate immediately.

Senator RUBIO. OK. My last question is for Facebook. It is about the geolocation data that is collected when people check in on the Places feature. Is this only collected at the time they check in?

Mr. TAYLOR. Right now, the Places feature is designed so you can explicitly share your location with people that you choose at the time of sharing. And so, Places is not a feature about passively sharing your location. It is about actively sharing your location.

Senator RUBIO. But that happens when you—at that moment, when you check in, basically. It is an active—it is an act of the——

Mr. TAYLOR. Yes, you actually click a button that says "check in," and that information goes on your profile.

Senator RUBIO. And then how long do you guys keep that information?

Mr. TAYLOR. That information that you shared, like "I am at this restaurant with some friends," that is on your profile as long as you want it to be. And you can remove it from your profile at any time.

Senator RUBIO. But if the individual doesn't remove it, it stays on there indefinitely?

Mr. TAYLOR. Yes. It is because we consider it just like if you published a status update on Facebook. It is you made the decision to share where you were, and it is up to you who you want to share it with and if you want to delete it. And you can actually change both of those after the fact.

Senator RUBIO. Right. By the way, you are probably not shocked that some people lie about where they are on their updates.

[Laughter.]

Senator RUBIO. I have seen that a few times. But, so people understand, when they go on there and they log on, they say, "I am here,"—that is going to stay on there forever unless you actively go back and delete it yourself?

Mr. TAYLOR. That is correct, and it is because, fundamentally, it is just like if you decide to share a status update or a photo, we consider that your information, not ours. And we consider it actually sort of an imperative to actually keep that information because you have entrusted us to keep it on behalf of, you know, sharing it with your friends.

Senator RUBIO. Thank you, guys. I appreciate it. Thank you.

Mr. TAYLOR. Thank you.

Senator PRYOR. Thank you.

Senator Thune?

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

Senator THUNE. Thank you, Mr. Chairman, and I want to thank all the panelists.

We are all encouraged by the substantial growth and the wonderful technology we have today in the mobile marketplace. But it does, you know, obviously raise questions and concerns about how the developing industry is impacting consumer protection and privacy. And so, having all these—access to all these things in the palm of your hand is a wonderful tool.

And then there is a lot of competition to create the new, best, greatest thing, which is part of our entrepreneurial spirit in America. But we want to make sure that when we do it, we do it in a way that does appropriately protect consumers online without stifling that innovation and growth.

So I want to direct a question, if I might, to Mr. Davidson, and it has to do with this FTC recently alleged that Google had violated the FTC Act inappropriately—by inappropriately collecting Gmail user information to populate Google's Buzz social network. According to the FTC, Google's action led to its Gmail users receiving contact with individuals whom they had serious concerns about.

Could you talk a little bit about how Google has responded to the FTC on that matter?

Mr. DAVIDSON. Absolutely. You know, as I said in my testimony, we hold ourselves to high standards on providing transparency and choice control to our users. And the situation that you allude to, where the launch of our Buzz product didn't meet those standards was very confusing for our users.

We think we have fixed it relatively quickly. In a matter of days, we had changed the product. But we had been in a longer conversation with the FTC about it afterwards and then, relatively recently, entered into a consent decree with them.

We have agreed to, for the next 20 years, put our money where our mouth is, and we have signed up for two major things here. One is really installing—instilling privacy by design, a process in our company for making sure that we are thinking about privacy from the earliest moments. And that is going to be something that is audited and assessed by an outside auditor and reported to the FTC every 2 years for the next 20 years.

The second thing is that we have agreed that we are going to get affirmative consent from users for any new sharing of information. And those are two very powerful things, and I think those are the kinds of things we said we would do and had agreed to do, but now we have got a consent decree with the FTC to show our users that we are going to do it for the next 20 years.

Senator THUNE. Do you think that some of those particulars that you talked about might be considered a best practice for other companies to consider?

Mr. DAVIDSON. You know, I think that is something probably better addressed to other companies. I know that there are a lot of different models out there. We think that this was the right thing for Google and for our users, and so we have adopted this agreement with the FTC. And I leave it to others to decide what is right for other companies.

Senator THUNE. OK. I am concerned that if companies agree to implement more restrictive privacy controls, that there are still individuals who are going to try and hack into mobile devices and apps to collect user information for third-party users. It just seems that mobile devices and apps are far more susceptible to hackers and to those types of deceptive activities.

And this is a question that any of you feel free to answer. Has the industry considered how they can make mobile devices and apps more secure, similar to how we, you know, protect our home computers with anti-virus software and firewalls, those sorts of things? And are we seeing any companies that specialize in security for mobile devices and apps?

Mr. Reed?

Mr. REED. On the first part of the question, yes. As a matter fact, there is a company called Lookout that is building a product for the Android platform that provides security and malware detection for the Android platform.

I mentioned the Android because it is a little different than Apple. Apple gives us as developers very little access to information of the device itself. They are very restrictive in what we in the developer community can ask for in terms of information.

So we—it is a little—it is where you see a lot more in the space, in the Android space, where it is more of the wild, wild West, and where there is more of a tendency for people to do the kinds of malfeasance that you are talking about. So Lookout is an example of a company that has come to the fore to address the problem that you have stated.

Mr. DAVIDSON. Yes, we would—so, first of all, I think there is a huge amount of energy being put into security. It is a great question.

You won't be surprised that I wouldn't characterize it as the wild, wild West.

[Laughter.]

Mr. DAVIDSON. I think, actually, our view is actually the openness of the platform and the fact that the code is open source is actually a major security feature because people around the world are able to look and assess the code and assess the system and the security architecture and test it all the time. And that means that we believe in—you don't get security with secrets anymore. You get security with openness.

The other thing is that there are a huge number of features, and we are among the people who are rolling these out, and they are being rolled out for the mobile platform, things like making sure that there is https encryption by default on major products like Google, like Gmail, and it is available on Search as well.

We have added a two-factor authentication on another system to Gmail. That means that a password is not enough. You might actually to have a device and a password, which I think for people who are really concerned about their mail products, this is really important.

And there are a lot of other companies who are rolling these kinds of things out as well. So it is a very important area, and there is a huge amount of research going into it and work going into it.

Senator THUNE. Is there anything that Congress can do to help encourage greater protection when it comes to mobile devices and apps, or would you rather we stay out of it?

[Laughter.]

Mr. DAVIDSON. Well, it is a rapidly evolving area, for sure. I think there has been discussion about data breach legislation. I think a lot of us, for example, would say that that is an area for consideration because there is such a patchwork of state laws.

But I would just recognize there is a huge amount of———

Senator Thune: It is already happening.

Mr. DAVIDSON. It is a very dynamic environment right now.

Senator THUNE. OK. All right. Thank you, Mr. Chairman.

Thank you all very much.

Senator PRYOR. Thank you. Thank you, Senator Thune, for being here and asking those great questions.

I want to thank all of the panelists for being here today. I know that when you look at the pleasantness scale, sometimes coming before the Senate is way down here. But thank you for being here and thank you for testifying.

And as much as we talked about today, we covered a lot of issues. I feel like we still are just kind of at the tip of the iceberg

here. There is just a lot more to know and to learn and for us to weigh through, and we certainly appreciate your all's input and your help as we go through this.

We are going to leave the record open for 2 weeks, and I am certain that several will have additional questions and want to do some follow-ups. I know I have a few. But we will leave that open for 2 weeks, and we would really appreciate you all working with the staff and getting that back to us in a timely manner.

Thank you for being here, and we will adjourn the hearing.

Thank you.

[Whereupon, at 12:29 p.m., the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF HON. KAY BAILEY HUTCHINSON,
U.S. SENATOR FROM TEXAS

Thank you, Mr. Chairman, for calling this hearing. Privacy is a very complex issue, and today's witnesses will help the Committee continue its education on this important subject.

This hearing will strengthen our understanding of the relationship between consumers and the many players that make up the mobile communications marketplace, including how personal information is collected and used by mobile devices and services.

It is important to ensure that we fully understand what the impact is on consumers who take advantage of mobile communications, and the relationship between the utilization of consumer data and the provision of advanced, often free services.

Mobile communication is a rapidly changing marketplace, where new technology is constantly advancing and overtaking previously groundbreaking technology. This is even truer in the mobile marketplace, where the last few years have seen an explosion of highly evolved and increasingly capable products.

For example, mobile apps really just surfaced in 2008, but as we will hear on our second panel, the number of available mobile apps will likely exceed 500,000 by the end of this year.

Each of these apps had to be developed, and that development brings economic benefits to our economy and the creation of jobs. Now more than ever, we should be encouraging sectors of our economy that show this kind of promise for continued job creation.

With these new technologies have come new and increased recognition of privacy concerns for consumers who use online products and services.

Consumers are understandably wary of products that they may not fully understand, and of what companies do with the information about consumers that they gather.

This concern has come to the forefront with several high-profile incidents involving collection of consumer information. The attention those incidents received has served to raise public awareness that their information may be collected and used.

This increased attention has also made many consumers more conscious about privacy policies and practices when utilizing new products and services.

The marketplace appears to be responding to those concerns. Some companies have already started taking steps to improve privacy policies so they will no longer be merely screens of complicated information that a consumer quickly clicks through to get to the next screen, or to the desired application.

Many consumers are more aware of data collection activities and are looking for how a company treats their data. As a result, privacy policies and robust protection policies have become a selling point for many new technologies.

It is a positive development that several industries are working to create self-regulatory guidelines and best practices related to consumer privacy.

In response to the FTC's call in 2009, the Digital Advertising Alliance created self-regulatory principles governing the collection and use of information online.

Also, a majority of Web browsers are implementing various methods to allow consumers to prevent their online activity from being tracked.

In the mobile space, there are already privacy safeguard certifications available for mobile apps, and the app community is coming together to create its own set of privacy guidelines.

This is how the market is supposed to work—a consumer concern was identified and industry is working to address that concern.

While it is probably to early to determine if these market developments will work to fully meet consumer privacy needs, it is also too soon to assume that they won't.

Another area of concern has been the impact that these new technologies have on children. As technology users become increasingly younger, we must be mindful of the special needs those users have and work to ensure their privacy is protected.

I am interested to hear from the FTC today about its ongoing review of the Children's Online Privacy Protection Act, and how that applies in the mobile space. It will also be helpful to hear from the companies on our second panel how they handle young customers, and what they do to ensure their privacy is protected.

One of the most effective means of protecting children is ensuring parents are educated about what their kids are doing. That can be a challenge in the technology space, as many of todays' kids know much more about mobile communications than their parents ever will.

There is a real need to provide parents with information that they can trust, that is easy to understand, and that is easy to apply in monitoring their children's activity.

I am interested to hear from all of our witnesses what they are each doing to promote consumer education, specifically for parents.

As legislators, we have an important role in shining light on and investigating important issues to consumers. I believe we are appropriately filling that role in relations to privacy, and commend the Chairman for his continued commitment to ensuring our Committee is educated about these issues.

It will be important going forward that we continue to learn about this complicated topic so we can better understand how this complex system works, and what the potential ramifications of any new regulatory action would be.

I want to thank all of our witnesses for being here today, and I look forward to a productive hearing.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN F. KERRY TO DAVID C. VLADECK

Question 1. What is your general impression of the legislation on privacy that has been introduced in Congress thus far?

Answer. Although the Commission has not taken a position on general privacy or Do Not Track legislation, legislation introduced to date, including the Commercial Privacy Bill of Rights, the Do Not Track Act of 2011, and the Do Not Track Kids Act of 2011, all represent significant progress in addressing important privacy concerns while ensuring continued robust development and growth of new services. I support the fundamental goals of each of these pieces of legislation, respectively, to improve transparency and consumer choice over information collection, use, and sharing practices, to provide transparency and consumer choice regarding tracking, and to provide privacy protections for children and teens.

Question 2. Your answer to this question is important for helping us frame the debate and how you view it. For the record, when a company or organization collects someone's information, do you believe that the information is at that point the collector's or is the collector simply a steward of people's information and that the people on whom information is collected should retain some rights and authority over that information?

Answer. The courts have not spoken on the issue of who owns this data. But regardless of who legally owns the data, we believe it is in both consumers' and business's interest for companies to maintain privacy-protective practices. Maintaining privacy protection can help build consumer trust in the marketplace. To achieve this goal, companies should not collect data unless they have a legitimate business need to do so; safeguard the data they maintain, in order to keep it from falling into the wrong hands; and dispose of it once they no longer have a legitimate business need to keep up. In addition, they should provide consumers with simple ways to exercise choices about privacy and make sure that their information collection and use practices are transparent.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN F. KERRY TO BRET TAYLOR

Question 1. What is your general impression of the legislation on privacy that has been introduced in Congress thus far?

Answer. At Facebook, we are constantly innovating to give people clear control over what they share and with whom. We believe that any legislative or regulatory proposal should protect both consumer privacy and the innovation of new products and services, which is essential to economic growth and job creation.

We are pleased, for example, that the Kerry-McCain legislation acknowledges that there is a difference between entities that have an established relationship with their users—a relationship that enables users to understand how their data is used and hold companies accountable for misuse—and those that may be gathering data without a consumer's knowledge or consent. We do, however, have some remaining concerns—for instance, how the bill defines "sensitive information" in a social media context where people are proactively sharing information about themselves; how limitations on "third parties" could restrict innovation and growth in our vibrant developer community; and how various provisions could impact important business partner relationships. We look forward to working with your office on these and other concerns to ensure that the bill encourages companies to advance users' understanding and control over their information while maintaining providers' and developers' ability to innovate.

There have also been a number of proposals in Congress that advocate a "do not track" feature. We have concerns about those proposals that focus on data collection limitations without regard to the nature of the business relationship and the intended uses of data. A properly crafted do-not-track proposal would focus on the data practices of entities that do not directly engage with users, and that thus are not accountable to them.

In addition, it is essential that any do-not-track implementation specifically define what kind of "tracking" is prohibited. Some collection of information might be defined as "tracking" under a legislative proposal, but might not be a practice that users would intend to block by expressing a do-not-track preference. For example, a website may use historical login data that it has collected for account security purposes: if our systems detect login attempts from Belarus for a Facebook account that is usually accessed from an IP address in Washington, D.C., the "tracking" that alerts us to that situation allows us to activate safeguards intended to ensure that the individual accessing the account is in fact the account owner. That "tracking" isn't problematic and shouldn't be blocked by a user's do-not-track preference; to the contrary, it's necessary to our efforts to provide a safe and secure service.

Question 2. Your answer to this question is important for helping us frame the debate and how you view it. For the record, when a company or organization collects someone's information, do you believe that the information is at that point the collector's or is the collector simply a steward of people's information and that the people on whom information is collected should retain some rights and authority over that information?

Answer. User privacy, safety, and control are at the center of every product decision at Facebook. People control when, how and with what friends, websites and applications they want to connect to share their data, and at any time, they can remove that data or break those connections. Users own the information they share on Facebook and they can download or delete their data, modify and review their privacy and sharing settings at any time, or delete their accounts.

Question 3. How would you compare what Senator McCain and I are proposing to the regime you operate under in Europe or other parts of the world?

Answer. We are pleased that your proposal attempts to strike a balance between user control and economic growth and innovation, both of which are essential. Although many privacy laws and regulations in Europe and elsewhere also seek this balance, we think the critical step made by your legislation is the recognition that context matters: a company that has established, direct relationships with its users should not be regulated in the same way as entities that collect data as third parties to a user-website relationship—entities without a direct relationship to the user who may be gathering data without the knowledge or consent of the user and without any user control over the data collected.

As I noted above, we look forward to working with you and Senator McCain to ensure that your bill strikes the critical balance between encouraging innovation and ensuring people have control over the information they share online.

Question 4. Mr. Taylor, in your testimony, you state that before you institute proposed changes to your privacy policy you put them for comment for your users and if a threshold of comments is reached, you put the changes out for a vote. And you state, "Time and again, Facebook has shown itself capable of correcting course in response to individual suggestions and we will continue to be receptive to that feedback." When you change your privacy policy, does it change how you use or how people can access information you have previously collected and if so, shouldn't that require an opt-in choice if there is any question that the change would have affected whether or not that person would have given you their information in the first instance?

Answer. At Facebook, we're continually creating innovative tools and experiences that deliver new and unique value and benefits. We bring this same spirit of innovation to communicating with users about our services and giving them tools to understand exactly how our service works; we want people on Facebook to be able make informed decisions about whether to use Facebook and what to share with their friends and the world around them.

As you noted in your question, before we institute changes to our privacy policy, we present the proposed changes to our users and offer them an opportunity to comment on them. If there is significant engagement on the proposal, we put it to a vote of all Facebook users; even if a vote isn't triggered by the comment process, we review and are receptive to the feedback we receive. We believe that this notice and comment process—which notifies people about proposed changes and gives them an opportunity to comment on them before they take effect—is unique in the industry.

We also recently announced—and invited feedback on—a new format for our privacy policy that we think can serve as a model for the industry. This new format involves interactive features, tips, and educational materials, all of which are designed to make our privacy policy not only informative and accurate, but easily understandable as well. So far, the feedback on this "privacy policy 2.0" has been overwhelmingly positive, and we expect to formally adopt that new format in the near future. Right now, these initiatives stand alone in the industry, but we hope that our efforts in this area—both our notice-and-comment process and our reformatted privacy policy—can serve as a model for other companies that, like us, want to go the extra mile in communicating with users about how they use information.

Most revisions to our privacy policy attempt to better explain our practices to users: as our products and services evolve, so do our notices. It is rarely the case that we would revise our privacy policy in a manner that would enable us to retroactively change the audience that can view information that has already been shared on Facebook. With that said, should a change materially alter something fundamental about how we access, collect, or use information that has previously been shared on Facebook, we would consider additional notice and consent mechanisms. This is a fact specific analysis, based on the practices and the services offered.

It is also important to note that outside the confines of our privacy policy, we routinely communicate how products work through "roosters" that update users about new or enhanced features either when the users arrive on Facebook or when they use a particular product. How these special messages are distributed—appearing on the top right corner of the homepage, through Facebook messages, through blog posts, or other communication channels—is a highly contextual, fact-specific question. But be assured that we don't hesitate to use those options when we determine that changes should be explained so that people understand the products we provide and any information sharing or use associated with those products.

Question 5. When a Facebook user visits one of your partner sites, say the *New York Times*, are they ever tracked on that website in a way that is not visible and known to them?

Answer. Privacy is a responsibility we share with our global community of users, advertisers, and the developers of applications and websites that connect to our Platform. As part of this shared responsibility, we believe that everyone who participates on the Facebook Platform should commit to the same robust standards of transparency and user control.

Your question specifically relates to websites that connect with the Facebook Platform. When a third party deploys a Facebook social plugin on its website, it does so to enable its viewers to link their on-site experience with their Facebook experience. These features allow users to interact and share in ways never before possible through Facebook technology that allows logged-in Facebook users to interact directly with Facebook while on the third party site. For direct interactions (*e.g.,* by clicking a like or recommend button), the user is interacting with Facebook the same way she would if she was on *facebook.com.* In cases where someone visits a third party site and does not "interact" with the social plugin, Facebook only uses collected information to generate anonymous or aggregate reports, which are used to learn more about the Internet and make our products and services better.

Facebook's terms prohibit website or application developers who integrate with the Facebook Platform from directly or indirectly transferring any Facebook user data to third parties such as ad networks, data brokers, and the like. Except for limited basic account information, which along with all data is subject to the developer's privacy policy, the data accessed through Facebook when a Facebook user connects to an application may only be used within the application unless the user provides express consent to the application.

Questions about any data collection or tracking that websites other than Facebook might engage in are, of course, best directed to those websites. The *New York Times*, for example, has a lengthy privacy policy that includes a comprehensive discussion entitled "What Information Do We Gather About You?" [1] When Facebook users visit the *New York Times* website, non-Facebook actions taken on the site—clicking ads or filling out forms, for example—are governed by the *New York Times*' privacy policies, not Facebook's. However, for our part, we require that developers that integrate with the Facebook Platform post and adhere to their own privacy policy that tells users what user data they are going to collect and how they will use, display, share, or transfer that data.

Question 6. Mr. Taylor, Facebook has grown to more than 600 million users. I don't think that there is another social network that comes close in terms of size and scope. Doesn't that mean that if you want to access this world of people with all the benefits you list, then you don't really have a choice just to switch to another social network if Facebook privacy practices cause you concern right?

Answer. People unquestionably have choice when it comes to connecting with others and expressing themselves online. Hundreds of millions of people use services other than Facebook to connect, to micro-blog, to share photos and other details of their lives, and to identify and consume content online and off. In the U.S., these services include Twitter, LinkedIn, MySpace, Diaspora, Picasa, Tumblr, Blogger, Wordpress, Path, Ping, Foursquare, Gowalla, and many others. Internationally, Orkut, Tuente, Studi VZ, V Kontakte, Ren Ren and a host of others are popular and growing quickly.

As recently as two years ago, MySpace was perceived to be the nation's leading social network and Facebook was the upstart. Virtually every day, the media reports news of another social media initiative—either from established technology companies such as Google or Apple, or from new, aggressive, and often well-funded competitors. Facebook, in short, operates in a robustly competitive environment that keeps us highly motivated to innovate and to continue providing people with services they find meaningful.

We have developed the Facebook Platform in a manner that enhances competition and fosters that motivation. As I explained in my testimony, the Facebook Platform is, at a conceptual level, modeled on the open architecture of the Internet. We permit—indeed, encourage—developers to launch applications that provide users with new and innovative social experiences, even where those experiences are similar to features we provide on *facebook.com.* To pick just one example, numerous location-sharing services—Foursquare and Gowalla, to name some—have integrated with the Facebook Platform, which has helped them grow. Those services directly compete with our own location-sharing service, and their presence on the Facebook Platform provides additional assurance that we will remain highly competitive and innovative. If we don't—not just in location sharing, but also in photos, messaging, micro-blogging, and other services—users will go elsewhere.

The same is true with respect to the privacy controls we provide to users. Facebook's mission is to make the world more open and connected. The explosive growth of Facebook and the many sharing sites listed above shows that people around the world believe in that goal as well: people want to share, they want to stay connected with their friends and families, and they want to feel connected to the world around them. We think that the best way to encourage that sharing is by giving users control over what and how they share, and with whom.

We care deeply about privacy, and we are continually innovating to make controls clearer, more direct, and easier to find and use. We think that's the right thing to do, and, at least as important, staying competitive demands it. If we stumble—either because our service is not engaging or because people believe they lack control—they will turn elsewhere. Although there are many other websites that offer social networking services, we are committed to leading the charge in the industry in how people control their information, and we think the user trust that results from that leadership is one of the key reasons we have been successful to date. People tacitly acknowledge these efforts with continued use of our product, and they explicitly acknowledge it too: an October 2010 study by TRUSTe indicated that the vast majority of parents and teens understand how privacy works on Facebook.

But as your question acknowledges, we can't please everyone. Although we think there are enormous benefits to being a part of our open and connected global network, those benefits are predicated on a willingness to share some basic information and connect with others. Some people are resistant to sharing and connecting online, and they may be uncomfortable with even the very limited mandatory informa-

[1] *http://www.nytimes.com/content/help/rights/privacy/policy/privacy-policy.html.*

tion that is displayed on every account. We feel that it isn't a lack of competition that prevents those individuals from enjoying the benefits of Facebook and other social media.

That said, as I mentioned before, we are always working to make our privacy controls more powerful and easier to use and understand, so that even people who may have reservations about sharing at the outset—or those with less sophisticated Internet and computer skills—feel comfortable on Facebook. That continuous improvement and user education are essential for our business in a competitive and rapidly changing market, and they are a critical part of our mission to make the world more open and connected.

RESPONSES TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN F. KERRY TO MORGAN REED

Question 1. What is your general impression of the legislation on privacy that has been introduced in Congress thus far?

Answer. Currently, Congress is considering at least 7 different privacy related bills, ranging from narrow bills dealing with just geolocation, to more comprehensive privacy efforts. Given the broad scope, it seems best to talk about the characteristics found in the legislation that are beneficial to our technology ecosystem, and those that may hinder us:

Most of the bills in Congress today take a technology focused, rather than data focused, approach. With the exception of the Kerry-McCain bill, nearly all other privacy legislation in the 112th Congress begins from the premise that new technology somehow requires new or different law. he fact remains that your location is tracked by the swipecard at the grocery store even though a smartphone with GPS was never used—and I am not required to "opt-in" anew every time use my customer card even though it is collecting my location data. Likewise, mail-order catalogs are often tailored to each recipient, despite any "opt-in" preferences or requests from the resident. We believe the holistic approach represented in Kerry-McCain is more effective, and does not disadvantage new technologies.

Many of the bills in Congress do not adequately address the need for FTC resources to enforce new provisions, at the same time the FTC is not even beginning to fully enforce existing privacy laws like COPPA. Since passage of COPPA in 2000, the FTC has brought roughly a dozen actions against high profile sites, barely more than one a year. Yet FTC's inaction has not been because the Web has become a perfectly compliant environment. Every child advocacy group could provide Congress a list of dozens of non-COPPA compliant sites run by legitimate organizations—the FTC simply lacks the resources to build a case and prosecute the violators.

Finally, some of the legislation, specifically bills addressing "Do Not Track" create technologically unworkable, and potentially deceptive problems. This is because a Do Not Track list is very different from the highly successful Do Not Call list. Since consumers have few phone numbers, and such numbers are static, it was easily implemented. On the other hand, a Do Not Track list requires the collection of information about every Web browser, mobile device, and application a consumer uses. This can be dozens if not hundreds of different identifiers. Furthermore, these are not static values in the same way a phone number is; consumers and developers can change and delete software cache and preferences. Also, FTC Commissioners have raised concerns that use of "Do Not Track" may be deceptive [1] since under a Do Not Call, the consumer receives no advertisements. However, under a Do Not Track, the consumer still sees ads, perhaps more ads, just not ones that are based on their interests.

We ask that when deciding how to proceed, you remember that the provision of many of the $1 or free applications available to users is predicated on the collection, use, and sharing of non-sensitive information by the default. We support a customers' right to opt-out of such collection, but many of the bills allow the FTC to determine the default for consent to the sharing of non-sensitive information with third parties. Since the FTC is on record as expressing that the default should be an "opt-in" to consent,[2] this would force apps developers to charge higher prices, provide less content, or even stop developing. Furthermore, the default opt-in requirement locks in existing businesses' control of the market while inhibiting new

---

[1] *See* FTC Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers*, Concurring Statement of Commissioner J. Thomas Rosch, page E–1.

[2] *See* Comments of Jessica Rich, Deputy Director of the FTC's Bureau of Consumer Protection on Google-Buzz Settlement.

entrants. Under an opt-in regime, established businesses can more easily completely consumers to opt-in to data sharing. And other large businesses like Google, can simply purchase third parties, making them first parties, completely circumventing any laws preventing third-party sharing.

Question 2. Your answer to this question is important for helping us frame the debate and how you view it. For the record, when a company or organization collects someone's information, do you believe that the information is at that point the collector's or is the collector simply a steward of people's information and that the people on whom information is collected should retain some rights and authority over that information?

Answer. The question of information ownership vs. information stewardship depends in large part on the type of information held. It is important to note that even within the context of information regarding an individual's use of a product, sensitive data (financial or health) is already governed by separate laws (GLB and HIPPA respectively).

Ownership confers a property right that often cannot truly be executed on information that may be in the public domain. It's like the old riddle, "What is very personal that you share with everyone and everyone else uses more than you? Your name." I can't ban its use by others, I can't stop people from calling it to me in public, yet I think most of us feel some level of possession over our name. Therefore information about a person is hard to structure in the same way we would "ownership" of the shovel that sits in my garage.

The courts, however, have determined that certain intellectual property rights do accrue to information about something or someone that has been merged with other data to create a new information product. Analysts can look at public business records and then combine that information with independent research to create a copyrightable product. Other court cases have addressed the ownership of customer lists, and the treatment of such data as an asset. Finally, FASB has rules governing the treatment of customer lists as an asset.[3] Therefore, we see information pertaining to how a consumer uses my product as the property of the business.

The product's creator is allowed to know and keep the information that you used the product, and what specifically you did while you were using the product. For example if it's a Web page, the developer of the page should be allowed to know what pages have been visited by what IP addresses, or for a mobile game developer to know what level you've finished. If the site or game provides for registering, then it is reasonable and fair for the product's creator to keep the information that "Jane@smith.com has made it to level 12".

The next category of information is "reference data." Information that might not be about the use of my product, but which companies are allowed to collect and maintain control. For example, you cannot be allowed to own information to the degree that you could remove just the problem areas in a credit report, or to submit a false address into the DMV. However, there is a need for the organizations and companies that collect "reference data" to keep the information accurate, and have reasonable procedures to correct data that is wrong. Companies in this regard may still own the data, but have greater responsibility to allow me to see the data they possess. For that reason, Congress has passed FCRA, GLB, HIPPA and other legislation that grants the person whose data is in question to play a part in ensuring accuracy.

One of the more interesting questions regarding "ownership" deals with location information. The news reports regarding the collection of GPS information on mobile devices is a bit unnerving, but do I "own" my location? If I am standing in front of the grocery store and a friend sees me, do I "own" that bit of information? When I use my grocery store swipecard inside the store, which stores the time of my purchase as well as the location of the store (and even the specific register I passed though), do I own that? In both cases the answer is no. When standing outside on the street, I have no expectation of privacy; I expect that others can see me. And when I sign up for a swipecard, I expect that the grocery store is going to collect, and even sell, the information. This example holds true for mobile devices. Apps that broadcast my location as part of their key functionality is the same as standing on the street—I expect that I will be seen, and even desire it. An app that uses advertising as the funding mechanism, and alerts me to the collection of location information, is like a swipecard that gives me discounted prices in exchange for my information.

Note that this information in question is often given to the recipient from the user in return for services from the recipient. For example, the a user will give the *Wash-*

[3] *FASB 141 (ASC 805)*

ington Post their e-mail address, zip code, gender, birth year, job industry, title, and responsibility in exchange for access to the *Washington Post's* content. In essence, the *Washington Post* is buying the rights to this content from the user for the price of the newspaper's content. Likewise, using a "Savings Card" at Safeway enables the store to collect information about users' buying habits and then resell that information. Safeway then gives some of the earned money back to consumers through discounted products.

By allowing this transaction, we allow users to monetize their personal information and trade it for goods and services.

Question 3. Mr. Reed, in your testimony you question the need for new legislation given the FTC's current authority and you argue against a new law that only targets app providers. I agree that our work should be comprehensive but have some questions for you about the adequacy of the FTC's current authority. Is it your opinion that app providers today are complying with fair information practice principles absent any new law?

Answer. Most apps developers are making best efforts to ensure the proper collection, use, and protection of consumers' data. They are undertaking this not primarily because of the legal ramifications, but more significantly the business implications that come with a breach of customer trust. Apps developers know that the trust of the their customers is paramount, especially with so many competitors in the market.

The focus of The United States Federal Trade Commission's Fair Information Practice Principles (FIPs) has always been on those who actually collect data, and independent research shows that the vast majority of mobile apps do not collect any personal data; thereby complying with FIPs. That said, some areas of data collection are unclear, and we all await the upcoming FTC rulemaking to help developers understand how best to follow the FIPs, for those apps developers who still need to improve their compliance, ACT is developing methods to assist them.

ACT is releasing this upcoming week its Privacy Policy Guidelines for Apps Developers. ACT will follow up with model privacy policies. Finally, ACT is creating a custom privacy policy generator for apps developers.

Question 3a. Does the FTC have the authority to mandate that app providers secure the information they collect or provide consumers with specific information about why that information is collected and how it will be used and distributed?

Answer. First, the information we are talking about here is non-financial, non-health information (that is already covered under GLB and HIPPA). So really, the question is, does the FTC have authority over non-sensitive information that apps developers collect.

I believe the FTC already has the requisite authority to ensure that apps developers properly treat the non-sensitive information they collect under section 5 of the FTC Act. This is supported by the FTC Staff Report—*Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers*—Concurring Statement of Commissioner J. Thomas Rosch:

> Moreover, Section 5 liability could not be avoided by eschewing a privacy notice altogether both because that would generally be competitive suicide and because that course would be deceptive in that it would entail a failure to disclose material facts.
>
> A privacy notice that is opaque or fails to disclose material facts (such as the fact that consumer information may be shared with third parties) is deceptive under Section 5. That is particularly true if the sharing of the information may cause tangible harm. Moreover, Section 5 liability could not be avoided by eschewing a privacy notice altogether both because that would generally be competitive suicide and because that course would be deceptive in that it would entail a failure to disclose material facts.

Therefore the FTC can and does already have the authority to ensure that data is properly protected, even when collected by apps developers.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN F. KERRY TO CATHERINE A. NOVELLI

Question 1. What is your general impression of the legislation on privacy that has been introduced in Congress thus far?

Answer. As we outlined in detail in our May 19, 2011 testimony, Apple has demonstrated an unwavering commitment to giving our own customers clear and transparent notice, choice and control over their personal information. Apple has adopted

a single comprehensive privacy policy for all its businesses and products, including the iTunes Store and the App Store. Apple's Privacy Policy, written in easy-to-read language, details what information Apple collects and how Apple and its partners and licensees may use the information. The Policy is available from a link on every page of Apple's website.

While Apple does not have a public position on any specific privacy legislation currently before the Congress, we do strongly agree that any company or organization with access to customers' personal information should give its customers clear and transparent notice, choice and control over their information. We have made this a strict licensing requirement for all of our app developers. We also share your concerns about the potential misuse of all customer data, and we believe that we have instituted policies and procedures that encourage third-party app developers to go well beyond disclosures written in an online privacy policy. Apple remains committed to working with the Congress, as well as with our technology industry colleagues and our trade associations in the private sector, to continue to identify the very best approaches for addressing consumer online privacy protections.

Question 2. Your answer to this question is important for helping us frame the debate and how you view it. For the record, when a company or organization collects someone's information, do you believe that the information is at that point the collector's or is the collector simply a steward of people's information and that the people on whom information is collected should retain some rights and authority over that information?

Answer. As stated in Apple's response to "Witnesses Question 1" above, Apple is committed to giving our customers clear and transparent notice, choice and control over their personal information. Apple agrees further that any company or organization with access to customers' personal information should give its customers clear and transparent notice, choice and control over their information. We have made this a strict licensing requirement for all of our app developers.

Apple has taken steps to help customers understand where their information is going and to provide customers with greater control over it. As stated clearly in our Privacy Policy, Apple makes it quite easy for our customers to access their own personal information provided to Apple. We provide our customers with secure access to their Apple account information to help ensure that the information is accurate, complete and up to date. We state clearly that we only retain information for the period of time necessary to fulfill the purposes outlined in our Privacy Policy unless a longer retention period is required or permitted by law.

Equally important, Apple takes precautions—including administrative, technical and physical measures—to safeguard our customers' personal information against loss, theft, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction. To make sure personal information remains secure, we communicate our privacy policy and security guidelines to Apple employees and strictly enforce privacy safeguards within the company.

Apple is always investigating new ways to improve our customers' experiences, including helping customers learn more about Apple's privacy policy and the privacy protections available on Apple mobile devices.

Question 3. Ms. Novelli, Apple has a good story to tell about the privacy protections it applies for its direct customers. In your testimony, you list 9 bullet points of privacy requirements that you impose on third party application developers for them operate on your platform. Is it your position that consumers do not have to worry about their information being distributed without their knowledge or consent by app providers because of the licensing agreement that those developers sign with you?

Answer. As we detailed in our May 19, 2011 testimony, Apple believes strongly that all third-party app developers with apps that collect information from users must provide clear and complete information to customers regarding the collection, use and disclosure of any user or device data. We not only make this mandatory in our licensing agreements, we also have documented in the App Store Review Guidelines a set of technical, content, and design criteria that every app must satisfy before Apple will accept the app for inclusion in the App Store. A copy of the Guidelines is attached to these responses.

Under these Guidelines, apps cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used. Further, we strictly prohibit the use of any analytics software in an application that collects and sends device data to a third party. Apps submitted to Apple for inclusion in the App Store that fail to meet these requirements are returned to the developer and are not offered in the App Store until the deficiencies are corrected.

Once an app is downloaded, the user's exchange of personal information within that app is between the user and the app developer. We make this clear in our privacy policy that once an app has been downloaded from the App Store, the information exchanged between the user and the app is governed by the privacy practices of the app's developer.

At the same time, Apple employees from several internal groups, or teams, are responsible for addressing issues that arise with apps that are available in the App Store. In addition to our own internal scrutiny, Apple relies heavily on communications from other App Store users, competitors, and industry observers to alert Apple of an app that is operating outside of Apple's Guidelines. Whenever such a case is brought to Apple's attention, either through internal vigilance or by an external party, Apple investigates and provides the developer with an opportunity to remediate. If no correction is made, Apple removes the app from the App Store.

Question 4. You state that as part of the licensing agreement, app developers have to explain their privacy practices to users yet both the WSJ and the Future of Privacy Forum have found that a significant percentage of app providers have no privacy policy at all. How do you reconcile those two facts?

Answer. As we stated in our May 19, 2011 testimony, Apple launched the App Store in July 2008 where customers may shop and acquire applications offered by third-party developers for the iPhone, iPad and iPod touch. As of June 6, 2011, the App Store includes more than 425,000 third-party applications covering a wide variety of areas including news, games, music, travel, health, fitness, education, business, sports, navigation and social networking. Because the overwhelming majority of these apps do not collect any information whatsoever from any user at any time, Apple has not mandated that its third-party developers incur both the legal expense and the burdensome administrative costs associated with issuing and maintaining a privacy policy unnecessarily—an expense that could well be prohibitive for a small struggling software developer or a teenager in his bedroom with only a MacBook and an idea.

For those apps that do collect information, however, our licensing agreement with developers prohibits any application from collecting user or device data without prior user consent. We also make it abundantly clear in our licensing agreement that developers, irrespective of size of business or age, must provide clear and complete information to users regarding their apps' collection, use and disclosure of user or device data. While many developers comply simply by adding a link to their online privacy policy, others have chosen to disclose this information by adding a pop-up dialogue box for the user to see when launching the app for the first time. We strictly prohibit the use of any analytics software in an application that collects and sends device data to a third party. Our licensing agreement also requires that apps comply with all applicable privacy and data collection laws and regulations regarding the use or transmission of user and device data, including location-based information. Apple's requirements are intended to provide the user with the most useful information that meets our strict transparency and disclosure requirements, but we also have chosen not to dictate the means by which that information is delivered to the user.

Because location information can be particularly sensitive, in addition to all the developer privacy and collection disclosure requirements described above, Apple has built a feature directly into the iOS that requires explicit customer consent when any application requests location-based information for the first time. When an application requests the information, a dialog box appears stating: "[Application] would like to use your current location." The customer is asked: "Don't Allow" or "OK." If the customer clicks on "Don't Allow," no location-based information will be provided to the application. This iOS dialogue box is mandatory—neither Apple's applications nor those of third parties are permitted to override it. For those customers that consent to allow an app to use their location information, an arrow glyph alerts them in real-time that an application is using or has recently used location-based information. Again, as we explained in more detail in our May 19, 2011 testimony, this consent for location services by an app can be given and rescinded on an app-by-app basis quite easily, and very transparently.

Question 5. Shouldn't all collectors of people's information be bound by fair information practice principles as a matter of law and if not, why not?

Answer. Once again, as we outlined in detail in our May 19, 2011 testimony and in response to Question 1 above, Apple clearly has demonstrated an unwavering commitment to giving our own customers clear and transparent notice, choice and control over their personal information. We believe our products do this in a simple and elegant way. While Apple does not have a public position on any specific privacy legislation currently before the Congress, we do strongly agree that any company

or organization with access to customers' personal information should give its customers clear and transparent notice, choice and control over their information. We have made this a strict licensing requirement for all of our app developers. We also share the Committee's concerns about the potential misuse of all customer data, and we believe that we have instituted policies and procedures that encourage third-party app developers to go well beyond disclosures written in an online privacy policy. Apple remains committed to working with the Congress, as well as with our technology industry colleagues and our trade associations in the private sector, to continue to identify the very best approaches for addressing consumer online privacy protections.

Question 6. In your testimony you state that Apple reviews all applications prior to adding them to the App store to ensure that they run properly and do not contain malicious code. Could you not also check whether they have a privacy policy with stated practices that comply with your licensing agreement?

Answer. Apple does check whether apps submitted for approval comply with the terms of our licensing agreement. For the reasons outlined in detail in our response to Question 4 above, Apple does not require a written privacy policy from developers when an app does not collect information from users. Again, for those apps that do collect information, Apple's app developer privacy requirements are intended to provide the user with the most useful information that meets our strict transparency and disclosure requirements, but we also have chosen not to dictate the means by which that information is delivered to the user.

Apple performs a rigorous review of every app submitted based on a set of technical, content and design criteria. The review criteria are documented in Apple's App Store Review Guidelines for iOS apps, which is made available to every app developer. The Guidelines include myriad requirements, including requirements about an app's functionality, and use of location or personal information. For example, the Guidelines state that:

4. Location

4.1 Apps that do not notify and obtain user consent before collecting, transmitting, or using location data will be rejected

. . .

4.4 Location data can only be used when directly relevant to the features and services provided by the app to the user or to support approved advertising uses

. . .

16. Objectionable content

16.1 Apps that present excessively objectionably or crude content will be rejected

16.2 Apps that are primarily designed to upset or disgust users will be rejected

. . .

17. Privacy

17.1 Apps cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used

17.2 Apps that require users to share personal information, such as e-mail address and data of birth, in order to function will be rejected

17.3 Apps that target minors for data collection will be rejected

. . .

18 Pornography

18.1 Apps containing pornographic material, defined by Webster's Dictionary as "explicit descriptions or displays of sexual organs or activities intended to stimulate erotic rather than aesthetic or emotional feelings," will be rejected

18.2 Apps that contain user generated content that is frequently pornographic (ex "Chat Roulette" alls) will be rejected

On average, Apple rejects approximately 30 percent of the apps initially submitted for consideration. The most common reasons for rejection relate to functionality issues, such as the app crashing, exhibiting bugs, or not performing as advertised by the developer. But Apple will reject an app for violating any of the criteria set forth in the Guidelines and/or any of the provisions of the developer's agreements with Apple.

When Apple rejects an app, most developers respond by correcting the issue or issues that led to Apple rejection so that the app may ultimately be accepted. Apple will not, however, accept any app in the App Store unless and until the developer and app are in full compliance with Apple's criteria and the developer agreements.

Similarly, Apple will remove from the App Store any app that is determined to be in violation of any of these requirements. Some of the most common reasons for

removal of an app from the App Store relate to an app's violation of some other party's intellectual property rights, violation of some law, or use of objectionable content.

[Apple's App Store Review Guidelines are offered below.]

App Store Review Guidelines

Introduction

We're pleased that you want to invest your talents and time to develop applications for iOS. It has been a rewarding experience—both professionally and financially—for tens of thousands of developers and we want to help you join this successful group. We have published our App Store Review Guidelines in the hope that they will help you steer clear of issues as you develop your app and speed you through the approval process when you submit it.

We view Apps different than books or songs, which we do not curate. If you want to criticize a religion, write a book. If you want to describe sex, write a book or a song, or create a medical app. It can get complicated, but we have decided to not allow certain kinds of content in the App Store. It may help to keep some of our broader themes in mind:

- We have lots of kids downloading lots of apps, and parental controls don't work unless the parents set them up (many don't). So know that we're keeping an eye out for the kids.
- We have over 350,000 apps in the App Store. We don't need any more Fart apps. If your app doesn't do something useful or provide some form of lasting entertainment, it may not be accepted.
- If your App looks like it was cobbled together in a few days, or you're trying to get your first practice App into the store to impress your friends, please brace yourself for rejection. We have lots of serious developers who don't want their quality Apps to be surrounded by amateur hour.
- We will reject Apps for any content or behavior that we believe is over the line. What line, you ask? Well, as a Supreme Court Justice once said, "I'll know it when I see it". And we think that you will also know it when you cross it.
- If your app is rejected, we have a Review Board that you can appeal to. If you run to the press and trash us, it never helps.
- If you attempt to cheat the system (for example, by trying to trick the review process, steal data from users, copy another developer's work, or manipulate the ratings) your apps will be removed from the store and you will be expelled from the developer program.
- This is a living document, and new apps presenting new questions may result in new rules at any time. Perhaps your app will trigger this.

Lastly, we love this stuff too, and honor what you do. We're really trying our best to create the best platform in the world for you to express your talents and make a living too. If it sounds like we're control freaks, well, maybe it's because we're so committed to our users and making sure they have a quality experience with our products. Just like almost all of you are too.

Table of Contents

20. Contests, sweepstakes, lotteries, and raffles
21. Charities and contributions
22. Legal requirements

1. Terms and conditions

1.1 As a developer of applications for the App Store you are bound by the terms of the Program License Agreement (PLA), Human Interface Guidelines (HIG), and any other licenses or contracts between you and Apple. The following rules and examples are intended to assist you in gaining acceptance for your app in the App Store, not to amend or remove provisions from any other agreement.

2. Functionality

2.1 Apps that crash will be rejected
2.2 Apps that exhibit bugs will be rejected
2.3 Apps that do not perform as advertised by the developer will be rejected
2.4 Apps that include undocumented or hidden features inconsistent with the description of the app will be rejected
2.5 Apps that use non-public APIs will be rejected
2.6 Apps that read or write data outside its designated container area will be rejected
2.7 Apps that download code in any way or form will be rejected
2.8 Apps that install or launch other executable code will be rejected
2.9 Apps that are “beta”, “demo”, “trial”, or “test” versions will be rejected
2.10 iPhone apps must also run on iPad without modification, at iPhone resolution, and at 2X iPhone 3GS resolution
2.11 Apps that duplicate apps already in the App Store may be rejected, particularly if there are many of them, such as fart, burp, flashlight, and Kama Sutra apps.
2.12 Apps that are not very useful, are simply websites bundled as apps, or do not provide any lasting entertainment value may be rejected
2.13 Apps that are primarily marketing materials or advertisements will be rejected
2.14 Apps that are intended to provide trick or fake functionality that are not clearly marked as such will be rejected
2.15 Apps larger than 20MB in size will not download over cellular networks (this is automatically prohibited by the App Store)
2.16 Multitasking apps may only use background services for their intended purposes: VoIP, audio playback, location, task completion, local notifications, etc.
2.17 Apps that browse the web must use the iOS WebKit framework and WebKit Javascript
2.18 Apps that encourage excessive consumption of alcohol or illegal substances, or encourage minors to consume alcohol or smoke cigarettes, will be rejected
2.19 Apps that provide incorrect diagnostic or other inaccurate device data will be rejected
2.20 Developers “spamming” the App Store with many versions of similar apps will be removed from the iOS Developer Program
2.21 Apps that are simply a song or movie should be submitted to the iTunes store. Apps that are simply a book should be submitted to the iBookstore.
2.22 Apps that arbitrarily restrict which users may use the app, such as by location or carrier, may be rejected

3. Metadata (name, descriptions, ratings, rankings, etc.)

3.1 Apps or metadata that mentions the name of any other mobile platform will be rejected
3.2 Apps with placeholder text will be rejected
3.3 Apps with descriptions not relevant to the application content and functionality will be rejected
3.4 App names in iTunes Connect and as displayed on a device should be similar, so as not to cause confusion
3.5 Small and large app icons should be similar, so as to not to cause confusion
3.6 Apps with app icons and screenshots that do not adhere to the 4+ age rating will be rejected
3.7 Apps with Category and Genre selections that are not appropriate for the app content will be rejected
3.8 Developers are responsible for assigning appropriate ratings to their apps. Inappropriate ratings may be changed/deleted by Apple
3.9 Developers are responsible for assigning appropriate keywords for their apps. Inappropriate keywords may be changed/deleted by Apple
3.10 Developers who attempt to manipulate or cheat the user reviews or chart ranking in the App Store with fake or paid reviews, or any other inappropriate methods will be removed from the iOS Developer Program

3.11 Apps which recommend that users restart their iOS device prior to installation or launch may be rejected
3.12 Apps should have all included URLs fully functional when you submit it for review, such as support and privacy policy URLs

4. Location

4.1 Apps that do not notify and obtain user consent before collecting, transmitting, or using location data will be rejected
4.2 Apps that use location-based APIs for automatic or autonomous control of vehicles, aircraft, or other devices will be rejected
4.3 Apps that use location-based APIs for dispatch, fleet management, or emergency services will be rejected
4.4 Location data can only be used when directly relevant to the features and services provided by the app to the user or to support approved advertising uses

5. Push notifications

5.1 Apps that provide Push Notifications without using the Apple Push Notification (APN) API will be rejected
5.2 Apps that use the APN service without obtaining a Push Application ID from Apple will be rejected
5.3 Apps that send Push Notifications without first obtaining user consent will be rejected
5.4 Apps that send sensitive personal or confidential information using Push Notifications will be rejected
5.5 Apps that use Push Notifications to send unsolicited messages, or for the purpose of phishing or spamming will be rejected
5.6 Apps cannot use Push Notifications to send advertising, promotions, or direct marketing of any kind
5.7 Apps cannot charge users for use of Push Notification
5.8 Apps that excessively use the network capacity or bandwidth of the APN service or unduly burden a device with Push Notifications will be rejected
5.9 Apps that transmit viruses, files, computer code, or programs that may harm or disrupt the normal operation of the APN service will be rejected

6. Game Center

6.1 Apps that display any Player ID to end users or any third party will be rejected
6.2 Apps that use Player IDs for any use other than as approved by the Game Center terms will be rejected
6.3 Developers that attempt to reverse lookup, trace, relate, associate, mine, harvest, or otherwise exploit Player IDs, alias, or other information obtained through the Game Center will be removed from the iOS Developer Program
6.4 Game Center information, such as Leaderboard scores, may only be used in apps approved for use with the Game Center
6.5 Apps that use Game Center service to send unsolicited messages, or for the purpose of phishing or spamming will be rejected
6.6 Apps that excessively use the network capacity or bandwidth of the Game Center will be rejected
6.7 Apps that transmit viruses, files, computer code, or programs that may harm or disrupt the normal operation of the Game Center service will be rejected

7. iAds

7.1 Apps that artificially increase the number of impressions or click-throughs of ads will be rejected
7.2 Apps that contain empty iAd banners will be rejected
7.3 Apps that are designed predominantly for the display of ads will be rejected

8. Trademarks and trade dress

8.1 Apps must comply with all terms and conditions explained in the Guidelines for Using Apple
8.2 Trademarks and Copyrights and the Apple Trademark List
8.3 Apps that suggest or infer that Apple is a source or supplier of the app, or that Apple endorses any particular representation regarding quality or functionality will be rejected
8.4 Apps which appear confusingly similar to an existing Apple product or advertising theme will be rejected

8.5 Apps that misspell Apple product names in their app name (*i.e.,* GPS for Iphone, iTunz) will be rejected
8.6 Use of protected 3rd party material (trademarks, copyrights, trade secrets, otherwise proprietary content) requires a documented rights check which must be provided upon request
8.6 Google Maps and Google Earth images obtained via the Google Maps API can be used within an application if all brand features of the original content remain unaltered and fully visible. Apps that cover up or modify the Google logo or copyright holders identification will be rejected

9. Media content

9.1 Apps that do not use the MediaPlayer framework to access media in the Music Library will be rejected
9.2 App user interfaces that mimic any iPod interface will be rejected
9.3 Audio streaming content over a cellular network may not use more than 5MB over 5 minutes
9.4 Video streaming content over a cellular network longer than 10 minutes must use HTTP Live Streaming and include a baseline 64 kbps audio-only HTTP Live stream

10. User interface

10.1 Apps must comply with all terms and conditions explained in the Apple iOS Human Interface Guidelines
10.2 Apps that look similar to apps bundled on the iPhone, including the App Store, iTunes Store, and iBookstore, will be rejected
10.3 Apps that do not use system provided items, such as buttons and icons, correctly and as described in the Apple iOS Human Interface Guidelines may be rejected
10.4 Apps that create alternate desktop/home screen environments or simulate multi-app widget experiences will be rejected
10.5 Apps that alter the functions of standard switches, such as the Volume Up/Down and Ring/Silent switches, will be rejected
10.6 Apple and our customers place a high value on simple, refined, creative, well thought through interfaces. They take more work but are worth it. Apple sets a high bar. If your user interface is complex or less than very good, it may be rejected

11. Purchasing and currencies

11.1 Apps that unlock or enable additional features or functionality with mechanisms other than the App Store will be rejected
11.2 Apps utilizing a system other than the In App Purchase API (IAP) to purchase content, functionality, or services in an app will be rejected
11.3 Apps using IAP to purchase physical goods or goods and services used outside of the application will be rejected
11.4 Apps that use IAP to purchase credits or other currencies must consume those credits within the application
11.5 Apps that use IAP to purchase credits or other currencies that expire will be rejected
11.6 Content subscriptions using IAP must last a minimum of 7 days and be available to the user from all of their iOS devices
11.7 Apps that use IAP to purchase items must assign the correct Purchasability type
11.8 Apps that use IAP to purchase access to built-in capabilities provided by iOS, such as the camera or the gyroscope, will be rejected
11.9 Apps containing "rental" content or services that expire after a limited time will be rejected
11.10 Insurance applications must be free, in legal-compliance in the regions distributed, and cannot use IAP
11.11 In general, the more expensive your app, the more thoroughly we will review it
11.12 Apps offering subscriptions must do so using IAP, Apple will share the same 70/30 revenue split with developers for these purchases, as set forth in the Developer Program License Agreement.
11.13 Apps that link to external mechanisms for purchases or subscriptions to be used in the app, such as a "buy" button that goes to a website to purchase a digital book, will be rejected
11.14 Apps can read or play approved content (specifically magazines, newspapers, books, audio, music, and video) that is subscribed to or purchased outside of the app, as long as there is no button or external link in the app to purchase the approved content. Apple will not receive any portion of the revenues for approved content that is subscribed to or purchased outside of the app

12. Scraping and aggregation

12.1 Applications that scrape any information from Apple sites (for example from apple.com, iTunes Store, App Store, iTunes Connect, Apple Developer Programs, etc) or create rankings using content from Apple sites and services will be rejected
12.2 Applications may use approved Apple RSS feeds such as the iTunes Store RSS feed
12.3 Apps that are simply web clippings, content aggregators, or a collection of links, may be rejected

13. Damage to device

13.1 Apps that encourage users to use an Apple Device in a way that may cause damage to the device will be rejected
13.2 Apps that rapidly drain the device's battery or generate excessive heat will be rejected

14. Personal attacks

14.1 Any app that is defamatory, offensive, mean-spirited, or likely to place the targeted individual or group in harms way will be rejected
14.2 Professional political satirists and humorists are exempt from the ban on offensive or mean-spirited commentary

15. Violence

15.1 Apps portraying realistic images of people or animals being killed or maimed, shot, stabbed, tortured or injured will be rejected
15.2 Apps that depict violence or abuse of children will be rejected
15.3 "Enemies" within the context of a game cannot solely target a specific race, culture, a real government or corporation, or any other real entity
15.4 Apps involving realistic depictions of weapons in such a way as to encourage illegal or reckless use ofsuch weapons will be rejected
15.5 Apps that include games of Russian roulette will be rejected

16. Objectionable content

16.1 Apps that present excessively objectionable or crude content will be rejected
16.2 Apps that are primarily designed to upset or disgust users will be rejected

17. Privacy

17.1 Apps cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used
17.2 Apps that require users to share personal information, such as e-mail address and date of birth, in order to function will be rejected
17.3 Apps that target minors for data collection will be rejected

18. Pornography

18.1 Apps containing pornographic material, defined by Webster's Dictionary as "explicit descriptions or displays of sexual organs or activities intended to stimulate erotic rather than aesthetic or emotional feelings", will be rejected
18.2 Apps that contain user generated content that is frequently pornographic (ex "Chat Roulette" apps) will be rejected

19. Religion, culture, and ethnicity

19.1 Apps containing references or commentary about a religious, cultural or ethnic group that are defamatory, offensive, mean-spirited or likely to expose the targeted group to harm or violence will be rejected
19.2 Apps may contain or quote religious text provided the quotes or translations are accurate and not misleading. Commentary should be educational or informative rather than inflammatory

20. Contests, sweepstakes, lotteries, and raffles

20.1 Sweepstakes and contests must be sponsored by the developer/company of the app
20.2 Official rules for sweepstakes and contests, must be presented in the app and make it clear that Apple is not a sponsor or involved in the activity in any manner

20.3 It must be permissible by law for the developer to run a lottery app, and a lottery app must have all of the following characteristics: consideration, chance, and a prize
20.4 Apps that allow a user to directly purchase a lottery or raffle ticket in the app will be rejected

21. Charities and contributions

21.1 Apps that include the ability to make donations to recognized charitable organizations must be free
21.2 The collection of donations must be done via a website in Safari or an SMS

22. Legal requirements

22.1 Apps must comply with all legal requirements in any location where they are made available to users. It is the developer's obligation to understand and conform to all local laws
22.2 Apps that contain false, fraudulent or misleading representations will be rejected
22.3 Apps that solicit, promote, or encourage criminal or clearly reckless behavior will be rejected
22.4 Apps that enable illegal file sharing will be rejected
22.5 Apps that are designed for use as illegal gambling aids, including card counters, will be rejected
22.6 Apps that enable anonymous or prank phone calls or SMS/MMS messaging will be rejected
22.7 Developers who create apps that surreptitiously attempt to discover user passwords or other private user data will be removed from the iOS Developer Program
22.8 Apps which contain DUI checkpoints that are not published by law enforcement agencies, or encourage and enable drunk driving, will be rejected

Living document

This document represents our best efforts to share how we review apps submitted to the App Store, and we hope it is a helpful guide as you develop and submit your apps. It is a living document that will evolve as we are presented with new apps and situations, and we'll update it periodically to reflect these changes.

Thank you for developing for iOS. Even though this document is a formidable list of what not to do, please also keep in mind the much shorter list of what you must do. Above all else, join us in trying to surprise and delight users. Show them their world in innovative ways, and let them interact with it like never before. In our experience, users really respond to polish, both in functionality and user interface. Go the extra mile. Give them more than they expect. And take them places where they have never been before. We are ready to help.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN F. KERRY TO ALAN DAVIDSON

Question 1. What is your general impression of the legislation on privacy that has been introduced in Congress thus far?

Answer. With respect to specific legislation, we salute the work of Senators Kerry and McCain to develop a comprehensive approach to privacy based on the same principles of transparency, control, and security we apply to our own services. We look forward to continued conversations about all of the privacy bills that have been introduced by members of the Committee as these bills evolve.

Google also supports ongoing Congressional work in two other areas which will strengthen Americans' privacy protections and provide consistency for providers. First, we applaud Congress' efforts to promote uniform, reasonable security principles, including data breach notification procedures, to ensure that the bad acts of criminal hackers or inadequate security on the part of companies do not undermine consumer trust for all services. Second, we support the efforts underway to update the Electronic Communications Privacy Act, the U.S. law governing government access to stored communications, to accord with the reasonable expectations of users of cloud computing services.

In general, Google supports the development of a comprehensive, baseline privacy framework that can ensure broad-based user trust and will support continued innovation. Key considerations for any such approach include even-handed application to all personal data regardless of source or means of collection, recognition of both the benefits and costs of legislating, particularly actual harm to users and compliance costs, and consistency of privacy rules across jurisdictions. In general, Google

does not favor a siloed approach to privacy law that focuses singularly on current technology or specific business models, such as location information or "Do Not Track" advertising privacy proposals. Instead, providers and consumers need consistent, baseline principles that will apply both to these issues and those to come in the future.

Question 2. Your answer to this question is important for helping us frame the debate and how you view it. For the record, when a company or organization collects someone's information, do you believe that the information is at that point the collector's or is the collector simply a steward of people's information and that the people on whom information is collected should retain some rights and authority over that information?

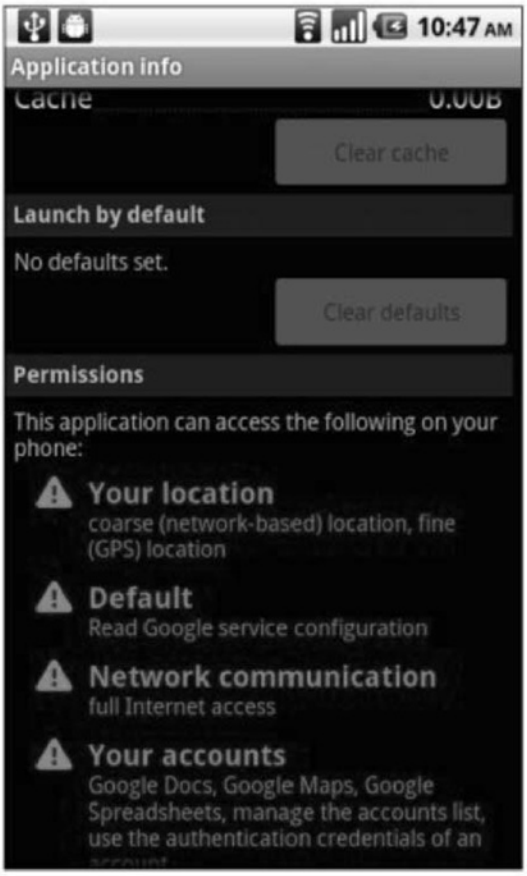
Answer. When you store your personal information online, we believe you should retain control of that data. This is why, for instance, we offer the Google Dashboard, (*www.google.com/dashboard*), to provide users with a one-stop, easy-to-use control panel to manage the use and storage of personal information associated with their Google accounts. In the Dashboard, a user can see, edit and delete the personally identifiable data stored with her individual Google account.

Providing our users with control over their personal information must also mean giving them the ability to take data with them if they decide to leave. In 2007 an engineering team at Google started the Data Liberation Front (*http://www.dataliberation.org*) to ensure that users are able to easily move their data in and out of Google products. The critical insight of the Data Liberation Front engineers was a recognition that users should never have to use a service unless they are able to easily retrieve the content they created with that service at no additional cost beyond what they're already paying for it. Starting with our Gmail service and now covering more than 25 Google products where users create and store personal information, these engineers have built tools to allow our users to "liberate" data if they choose to switch providers or to stop using one of our services.

Data portability has benefits for our users and for Google. First, our product teams know just how easy it is for their users to move to a competitor's product, and understand that their success depends upon continuing to be responsive to privacy and product concerns and acting quickly to address them. Second, allowing our users the freedom to leave honors our commitment to put users in control. We believe that this kind of "user empowerment by design" is an effective means of ensuring respect for user privacy without chilling innovation.

Question 3. In your testimony, you state that location sharing on Android devices is strictly opt-in for your users, with clear notice and control. You go on to state that is how location services should work. Do the application providers using the Android platform share that belief and why can't you require them to comply with that principle?

Answer. While we cannot speak on behalf of application developers, Google indeed requires every Android application to obtain the consent of the user prior to enabling access to location data via the device. The Android operating system uses a permissions model in which the user is automatically informed of certain types of information an application will be able to access (see the figure of the permissions screen below). An application can only access the device's GPS location or the device's network location if it displays a notice for this permission to the user at time of installation. The user may choose to trust the application by completing the installation or the user may choose to cancel the installation. However, the Android platform does not have the ability to control the behavior of third party developers or how they handle location information and other user information that the third party application obtains from the device.



In addition to the permissions structure of Android, developers that upload applications to the Android Market must agree to the Android Market developer agreement (*http://www.android.com/us/developer-distribution-agreement.html*), pursuant to which developers agree to comply with applicable laws and to protect the privacy rights of users. The specific relevant language is as follows:

> *4.2 You agree to use the Market only for purposes that are permitted by (a) this Agreement and (b) any applicable law, regulation or generally accepted practices or guidelines in the relevant jurisdictions (including any laws regarding the export of data or software to and from the United States or other relevant countries).*
>
> *4.3 You agree that if you use the Market to distribute Products, you will protect the privacy and legal rights of users. If the users provide you with, or your Product accesses or uses, user names, passwords, or other login information or personal information, you must make the users aware that the information will be available to your Product, and you must provide legally adequate privacy notice and protection for those users. Further, your Product may only use that information for the limited purposes for which the user has given you permission to do so. If your Product stores personal or sensitive information provided by users, it must do so securely and only for as long as it is needed. But if the user has opted into a separate agreement with you that allows you or your Product to store or use personal or sensitive information directly related to your Product (not including other products or applications) then the terms of that separate agreement will govern your use of such information. If the user provides your Product with Google Account information, your Product may only use that information to ac-*

cess the user's Google Account when, and for the limited purposes for which, the user has given you permission to do so.

Android Market is built on the principle of openness, with the goal of encouraging innovation and user choice. With this principle in mind, Google does not pre-screen applications before they are made available by developers to users of Android Market. But we will remove applications when we are notified about, or otherwise discover, applications that violate our developer agreement or policies. As of May 31, 2011, Google is removing an average of 250–300 applications per day from Android Market due to violations of our developer agreement or policies.

Google also strongly encourages application developers to use best practices for handling user data (*http://android-developers.blogspot.com/2010/08/best-practices-for-handling-android.html*), including recommendations that developers publish privacy policies and give users choice regarding data collection.

Many Android applications, however, are offered via other application stores or directly from the developers' websites. Since these applications are not offered through the Android Market, their developers are not subject to the Android Market developer agreement. But the permissions model described above and in our testimony would still apply (as this is a technical function of the Android operating system).

Note that because of the open source nature of the Android operating system, a device manufacturer can modify the Android operating system and can build an Android device without any involvement by Google. The response to this question and the questions below only relate to unmodified versions of the Android operating system as released by Google.

Question 4. In your testimony, you state that all applications using the Android operating system are prohibited from collecting user location information without the user's consent and without the user being informed of the types of information an application will be able to access. But then you go on to say that Google "does not and cannot control the behavior of third party applications." If you can control that they get consent and inform users on what is being collected, why can't you require them commit to not transferring that information to third parties without consent or require them to place reasonable retention limits on the information they collect or apply any of the other fair information practice principles?

Answer. As we discussed in the previous answer, the Android operating system uses a permissions model in which the user is automatically informed of certain types of information an application will be able to access. Once that permission is granted however, the operating system does not have the ability to control the behavior of third party developers or how they handle location information and other user information that the third party application obtains from the device.

While there is no technical means of limiting the use of data collected by application developers, as discussed above, developers that upload applications to the Android Market must agree to the Android Market developer agreement, pursuant to which developers agree to comply with applicable laws and to protect the privacy rights of users.

Question 4a. If you are not going to take responsibility for non-Google owned and operated application providers, shouldn't they as well as you, be subject to some legal code of conduct to ensure fair information practice principles are respected?

Answer. As discussed above, Google supports the development of a comprehensive privacy framework that applies baseline principles uniformly across entities that collect personal data and across jurisdictions. We look forward to working with the Committee and others in Congress on this issue.

In the meantime, Google strongly supports the development of codes of conduct and other mechanisms to push application developers to adopt practices that preserve user privacy and engage in responsible data collection and use. The mobile application industry can and should model the self-regulatory effort in the online advertising and publishing industries, which brought together hundreds of stakeholders to create uniform, enforceable standards for notice and control over targeted ads. Google has been deeply involved in that effort, and similarly hopes to work with other platform companies, app developers, and mobile carriers to better ensure transparency, user control, and security in this nascent industry.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN F. KERRY TO AMY GUGGENHEIM SHENKAN

Question 1. What is your general impression of the legislation on privacy that has been introduced in Congress thus far?

Answer. Common Sense Media is gratified to see the growing amount of focus that legislators in both chambers and on both sides of the aisle are bringing to this crucial issue.

Privacy is important to all Americans, but we believe it is especially important for kids and teens. So while we appreciate the focus on overall privacy rights, we would also like to see more emphasis on parents' rights to protect the privacy of their children, and on better tools and information that will help parents exercise those rights.

Question 2. Your answer to this question is important for helping us frame the debate and how you view it. For the record, when a company or organization collects someone's information, do you believe that the information is at that point the collector's or is the collector simply a steward of people's information and that the people on whom information is collected should retain some rights and authority over that information?

Answer. Our personal information belongs to each of us. We may authorize a company or organization to use our personal information, but it remains ours, and those companies or organizations have an obligation to be careful stewards of our information. Unfortunately, too many companies have demonstrated lately that they are not careful stewards, and that needs to change.

PREPARED STATEMENT OF FRAN MAIER, PRESIDENT, TRUSTE

Chairman Pryor, Ranking Member Toomey, and distinguished members of the Subcommittee—my name is Fran Maier, and I am President of TRUSTe, the world's leading provider of online privacy solutions. On behalf of TRUSTe, I applaud the Subcommittee's efforts and inquiries around protecting consumer privacy in today's mobile marketplace, as this is a topic that continues to present challenges for American consumers and companies providing products and services in the mobile ecosystem. We appreciate the opportunity to provide testimony on the issues, as well as results from two research studies that TRUSTe recently conducted, and that may be of interest:

- TRUSTe's survey of 1,000 smartphone users, conducted together with Harris Interactive, that focuses on user attitudes toward smartphone privacy.[1]
- TRUSTe's analysis of data collection from a sample of the 300 most popular apps on the Android, Apple and Blackberry mobile platforms (copy attached)

At TRUSTe, our focus is providing clients with a self-regulatory framework that both enhances incentives and encourages innovation around the commercial collection and use of consumer data. Based in San Francisco, California, we were founded as a non-profit, industry association in 1997. In 2008, we converted to for-profit status, with venture investment. Today, we certify the online privacy practices of over 4,000 web properties across a variety of platforms and services—including mobile. We provide privacy solutions to companies of all sizes—from smaller websites to larger companies with multiple brands and online properties.

TRUSTe supports the recommendations of the FTC and the U.S. Department of Commerce around the importance of developing a self-regulatory framework for online privacy. We believe that a self-regulatory model, if articulated correctly, is best equipped to deal with the privacy challenges posed by the complexity of business models in the online and mobile ecosystems.

Self-regulation works because it is agile enough to address the complexity of business practices in dynamic industries—like technology—while also preserving incentives for competition and innovation in a diverse ecosystem. TRUSTe, like other self-regulatory organizations, can detect lapses in the system, when they occur, and work directly with a company to resolve them. We also guide companies toward more sustainable and consumer-friendly business practices helping them re-evaluate and, in some cases, alter their current product strategies and implementations.

---

[1] TRUSTe recently released the results of a nationwide Harris Interactive survey of one thousand smart phone users, concerning privacy and use of mobile applications and mobile websites. More details at: *http://www.truste.com/why__TRUSTe__privacy__services/harris-mobile-survey/*.

At the end of the day however, we also believe that a successful self-regulatory program should work in tandem with government regulation. TRUSTe works closely with the FTC and other government agencies; proactively, around the launch of new products and services and in certain rare cases, enforcement referrals.[2] We also think it is important to have strong regulatory enforcement, especially in cases where companies willfully disobey self-regulatory requirements to the detriment of consumers.

TRUSTe's approach to self-regulation starts with our Program Requirements, which form the basis of our privacy seal program. Only sealholders and clients who are successfully certified under these requirements get to display the TRUSTe seal on their e-mails, downloads, mobile applications, and websites (we have provided some details about our certification process later in this testimony). In addition, we continue to evolve our Program Requirements in response to regulatory changes, as well as best practices and technological advancements on the desktop and mobile web.

Earlier this year, we announced major updates to our Program Requirements that better address the innovative changes and newer business practices we've seen in media and web technologies over the past few years: online behavioral advertising, mobile apps and marketing and social networking.[3] We worked closely with our clients, including several launching new products and services, to incorporate these updated privacy requirements into their existing privacy compliance. These updates to TRUSTe's Program Requirements exemplify why self-regulation works; at a time when privacy compliance standards remain in flux, it's important to have a framework that is both agile and relevant enough to provide a company the guidance (and confidence) it needs to engage customers and expand business opportunities.

TRUSTe has also observed robust growth in the market for self-regulation during the past year, and believe there are significant opportunities for self-regulatory compliance- on both the mobile and desktop web. During the past year, TRUSTe has launched three new privacy solutions—addressing Online Behavioral Advertising notice and choice to consumers,cloud applications and, most relevantly, mobile certification. TRUSTe is now the largest provider of the DAA's Self-Regulatory Program for Online Advertising through its TRUSTed Ads[4] program, which was just launched earlier this year. TRUSTed ads now serves more than 10 billion advertising choice icon impressions per month, and delivers online behavioral advertising notice and choice to consumers.

In the following sections, I provide some more details about TRUSTe—our guiding philosophy, as well as more details about our web seal and mobile certification processes.

Truth in Privacy

Essentially, the TRUSTe philosophy is "Truth in Privacy"—a concept that incorporates transparency, choice and accountability, and which aims to bring confidence to all stakeholders—businesses, consumers and governments—who view the TRUSTe seal.

For consumers, Truth in Privacy means:

- Accurate and comprehensive disclosures about personal information collection and/or use, that are readily accessible and in an easy to understand format
- Accessible choices and tools to help users proactively set personal information boundaries
- Direct, meaningful contact between the consumer and either the client/seal holder or TRUSTe, to resolve privacy concerns.

A recent TRUSTe/TNS brand survey shows that the TRUSTe seal gives consumers confidence—a site that displays the TRUSTe seal will follow its stated privacy practices.[5] In some cases, the presence of a TRUSTe seal was a deciding factor in whether the user wanted to share personal information with a site (or not). And,

---

[2] For instance, in 2008, we referred the case of Classic Closeouts to the FTC.

[3] *Updates to TRUSTe's Privacy Seal Program*, available at: *http://www.truste.com/privacy-program-requirements/*.

[4] TRUSTe is now the largest provider of the Digital Advertising Association's Self-Regulatory Program for Online Advertising, serving over 100 billion impressions per month. For more details, visit: *http://www.truste.com/privacy__seals__and__services/enterprise__privacy/trusted-ads.html*.

[5] TRUSTe—2009 TNS brand survey.

over 92 percent of consumers that used TRUSTe's Watchdog resolution mechanism stated that they would recommend the service to a friend.[6]

Truth in Privacy also has significance for our clients and sealholders. Displaying the TRUSTe seal means that the client or seal holder is:

- Developing privacy practices that align with leading industry standards and governing laws
- Providing & honoring consumer choices on personal information collection & use
- Innovating around privacy—developing "best of breed" privacy notices, etc.
- Being accountable for stated privacy promises (privacy policy, notice, etc.).

Governments also recognize the TRUSTe seal as a symbol of consumer safety and regulatory compliance, both here in the U.S. and internationally. In 2000, TRUSTe became a provider of the EU Safe Harbor Privacy services as outlined by the U.S. Department of Commerce and the European Union, and we are now the largest provider of EU Safe Harbor dispute resolution services. In 2001, the Federal Trade Commission approved TRUSTe's COPPA[7] Kid's Seal Program as an authorized safe harbor under the Children's Online Privacy Protection Act; today, we are the largest COPPA provider.

TRUSTe Core Program Requirements & Web Seal Certification

TRUSTe's web seal certification program is a voluntary, self-regulatory program. Clients and sealholders are first certified against a core set of Program Requirements, and then have the option to get additional certification in other areas, including mobile privacy.

TRUSTe charges companies for web privacy certification based on a number of factors, including the size of the organization (either measured by revenue or pages served), the complexity of their web property 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 data collected and the number of TRUSTe certification programs they use (Mobile certification, EU Safe Harbor certification, COPPA certification, etc). Thanks in part to technology such as our "automatic privacy policy generator," TRUSTe is able to deliver cost-effective services to small companies. In our experience, however, risk does not always correlate to size; a very small business can have incredibly complex data collection and management practices, while very large companies can sometimes have very simple data practices that may not even entail the collection or use of sensitive information.

TRUSTe certification begins with a direct evaluation of the website or application being certified, as well as the attestations and representations made by the company seeking certification. To supplement our direct evaluation and client attestations, TRUSTe employs monitoring technologies that verify compliance *e.g.,* scanners that confirm whether cookies are being dropped, whether age information is being collected, and whether changes are being made to privacy policies. We also employ e-mail seeding and https-encryption of sensitive information during transmission, traffic analysis, etc. While our focus is privacy compliance, our certification process has also helped certain clients and sealholders become aware of important security vulnerabilities in their data collection and use systems.

TRUSTe generally looks at the context of a practice—what type of data is being collected and with whom is it being shared—before determining the privacy obligations for that practice. For consent, the requirements for our website and mobile seal are the same, and differ whether the use is by first or third parties. Our Program Requirements include specific requirements around notice and choice: express or opt-in consent is required for all collection of "sensitive" data (we classify financial, medical and geo-location data as sensitive). We also require express consent for third party sharing, when the sharing is for the third party's secondary use. Finally, our Program Requirements acknowledge the growing reality that companies need to be transparent about all data collection, not just personal data collection, because discrete data elements (while lacking identifying characteristics on their own) can be used in combination to personally identify consumers.[8]

---

[6] TRUSTe monitors compliance by clients and sealholders through its consumer complaint mechanism known as Watchdog. The Watchdog Dispute resolution mechanism is extremely successful; in a 2010 TRUSTe survey, 92.3 percent of consumers that used Watchdog stated that they would recommend the service to a friend.

[7] "COPPA" refers to the Children's Online Privacy Protection Act of 1998, specifically the provisions around safe harbor.

[8] This is a forward thinking perspective that was advanced by FTC staff in their recent report. Specifically, staff noted the "the blurring of the distinction between personally identifiable infor-

Continued

TRUSTe knows that for the most part, our clients and sealholders want to elevate trust in their brand through exemplary privacy practices. In the dynamically changing world of the desktop and mobile web, this is always an evolving process. Nearly all of our clients and seal holder applicants will make changes to their existing practices to qualify for TRUSTe certification. In some cases, making these changes isn't enough for certification; in 2010, over 7 percent of applicants for our enterprise certification (those that are not using our more automated privacy policy and certification program aimed at smaller businesses) did not qualify for TRUSTe certification because they did not meet our rigorous certification standards.[9] TRUSTe also retains the option to decline certification 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.

TRUSTe closely reviews and monitors all business practices prior to certification, and checks them again annually upon renewal by the client or seal holder. In addition, clients and sealholders are required to contact TRUSTe in advance of making material changes to their privacy policies or business practices. We initiate compliance investigations based on certain events, such as:

- monitoring events resulting from TRUSTe's scanning technology or our independent e-mail seeding of a client or sealholders' e-mail lists
- receiving a Watchdog dispute resolution complaint from a consumer
- press, news reports, regulatory hearings and reports.

At TRUSTe, we generally reach out to the client and seal holder when we first learn of an issue. In some cases, we may precede this initial contact with an own independent investigation to determine if the issue can be reproduced. In our experience, TRUSTe clients and sealholders generally acknowledge and fix issues promptly. In some cases, we find that issues are addressed prior to TRUSTe's learning of it. Depending on the nature of the issue, the client or seal holder's good faith and timely responsiveness, and the timing of expected resolution for an issue, TRUSTe may choose not to resort to a formal enforcement process *e.g.,* if the issue is fixed before the cure period completed. As TRUSTe's privacy solutions are voluntary programs, clients and sealholders may choose to terminate certification at any time—unless TRUSTe has initiated a formal enforcement proceeding against the client and that proceeding remains unresolved.

To preserve incentives for privacy certification, TRUSTe believes that appropriate confidentiality and due process (including the opportunity to cure) must be an integral part of any self-regulatory framework. Our formal enforcement process consists of three stages:

1. *TRUSTe investigation*—including outreach to the client or seal holder in question

2. *Suspension* with opportunity to cure—Depending on the results of the TRUSTe investigation, the client or seal holder will be given suspended from the certification program, with the opportunity to cure within an allotted time

2. *Termination*—If the client or seal holder does not cure the issue within the allotted time, TRUSTe will issue a Termination for Cause, and end its certification of the client or seal holder in question.

Depending on the nature of the violation, TRUSTe may take additional steps such as publishing the termination and/or referring the issue to the attention of a regulatory or other governmental agency, including the FTC. Our of our prior FTC referrals was ClassicCloseouts in 2008; we assisted the FTC with the investigation, and they brought action for permanent injunction and relief against the site, ultimately obtaining a $2.08 million settlement to provide redress for consumers.

TRUSTe Mobile Certification

TRUSTe's mobile privacy certification program helps companies successfully use technologies such as geo-location, advertising, and social networking to improve consumer adoption of their platforms and mobile apps.[10] Clients or sealholders seeking

---

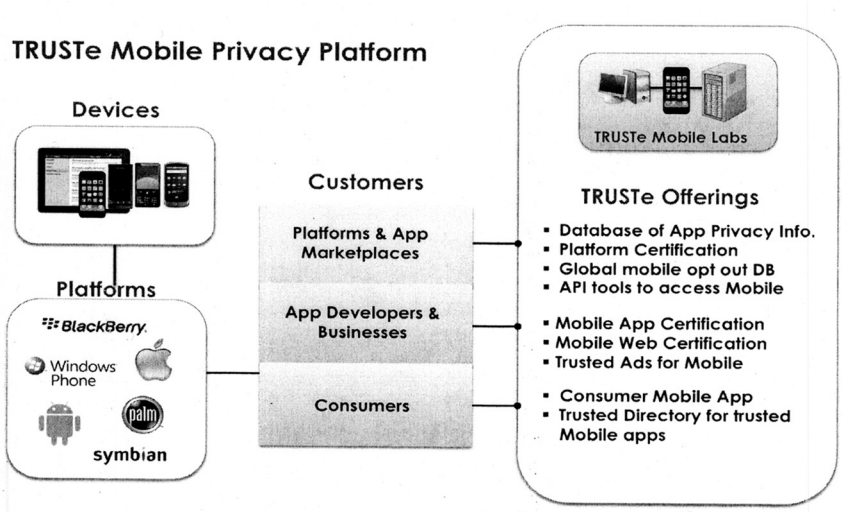
mation and supposedly anonymous or de-identified information. FTC Staff Report, Protecting Consumer Privacy in an Era of Rapid Change (2010), available at: *http://www.ftc.gov/os/2010/12/101201privacyreport.pdf*.

[9] The exact figure is 7.4 percent—out of a total of 2611 TRUSTe clients and sealholders, 193 did not complete certification in 2010.

[10] More details about TRUSTe mobile privacy certification are available at: *http://www.truste.com/privacy__seals__and__services/enterprise__privacy/mobile__certification.html*.

mobile certification will first need to comply with our core Program Requirements. The specifics of our projected mobile privacy certification platform are illustrated in Figure 1, below. We hope to deploy all of these certification services within the next few months.

Figure 1—TRUSTe's Mobile Privacy Platform



Under the TRUSTe mobile certification process (and similar to our process for web seal certification), we first review all business practices of a mobile web or applicationsite to determine eligibility for certification. Once certification is granted, TRUSTe verifies compliance with our program requirements through a combination of scanning and seeding technology that looks for specific privacy "markers" *e.g.,* are cookies, beacons, scripts or other types of targeting or tracking technology being used, what kind of information is being collected and is sensitive information being protected. We also perform a thorough review of the mobile app or website's privacy policy, if available and will require that companies modify their privacy statement to reflect current data management practices. For mobile apps specifically, we perform a data packet analysis; we analyze data transfers to/from the app (and where needed, test for secure transfers), confirm data collection practices and identify third party data-sharing and transfers.

Similar to our web seal certification process, TRUSTe generally looks to the context of a practice—what type of data is being collected by the mobile app or website, is it for first party or third party use, etc.—before determining the privacy obligations for that practice. Sensitive data that is collected for first-party use requires a consumer's express consent before it is shared with third parties.[11] Under TRUSTe's web seal and mobile certification programs, we classify geo-location data as sensitive data. This means that TRUSTe clients and sealholders must get a user's express or opt-in consent before sharing that data with third parties, including third party application developers.

TRUSTe also requires notice for all third party data collection and use on a mobile device. For collection and use of sensitive data by third parties, the consumer's express consent must be obtained. For non-sensitive data that will be shared with third parties, a consumer must be given notice that the data is going to be shared—either through a link to a privacy policy at the point of collection, or a check box at the point of collection. If a TRUSTe client or seal holder plans to share a consumer's personal information with third parties for unexpected purposes, they are also required to provide a Just-in-Time notice and opt-out mechanism.

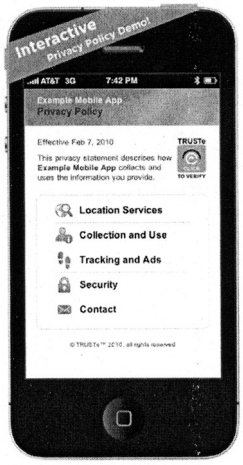
TRUSTe has also been at the forefront of creating innovative solutions that help our clients and sealholders address the challenge of presenting a comprehensive privacy notice on the small screen. For instance, our mobile short notice format uses a mix of icons and text to address key privacy concerns such as the collection and

[11] In contrast, we require non-express or "opt-out" consent for first party collection of non-sensitive data for the first party's use.

use of geo-location information on a mobile device. We have provided two examples of our mobile short notice, in Figures 2 and 3 below.

Figure 2—TRUSTe Mobile Short Notice for Location Services using Geo-location data

Figure 3—TRUSTe Mobile Short Notice Showing Purposes for Data Collection



Currently, examples of TRUSTe certified mobile applications include:

Breastcancer.org (iPhone)
Callvine (iPhone)
Lookout (Android)
Worldmate (Blackberry, mobile web)

TRUSTe—Harris Interactive Mobile Privacy Survey

As the Subcommittee knows, TRUSTe and Harris Interactive recently conducted a nationwide survey of 1,000 smartphone users that focused on mobile privacy.[12]

[12] See TRUSTe: Mobile Privacy User Results, available at: *http://www.truste.com/why__TRUSTe__privacy__services/harris-mobile-survey/*.

The survey provides important data about consumers' mobile privacy attitudes and concerns, while also identifying areas where mobile app and operating system developers could do more to provide increased privacy protections for consumers. Given the lack of relevant research on consumer mobile privacy, TRUSTe had a particular interest in conducting the survey: we serve consumers and we wanted to know their concerns, so that we could inform our clients and sealholders accordingly, while also making necessary revisions to our recently launched mobile privacy certification program.

The key findings of the TRUSTe-Harris survey are illuminating. The vast majority of respondents (98 percent) believed that privacy is important when using smart phones—in fact, more than 1 in 3 of the respondents (38 percent) identified privacy as their number one concern when using mobile applications, followed by security (26 percent) and identity tracking (19 percent). Most respondents remain concerned about targeting and tracking technologies on smart phone devices—particularly those that collect geo-location data. And, despite increased adoption of smart phones in recently years, 1 in 3 respondents felt that they were in less in control of their personal information with a smart phone device.

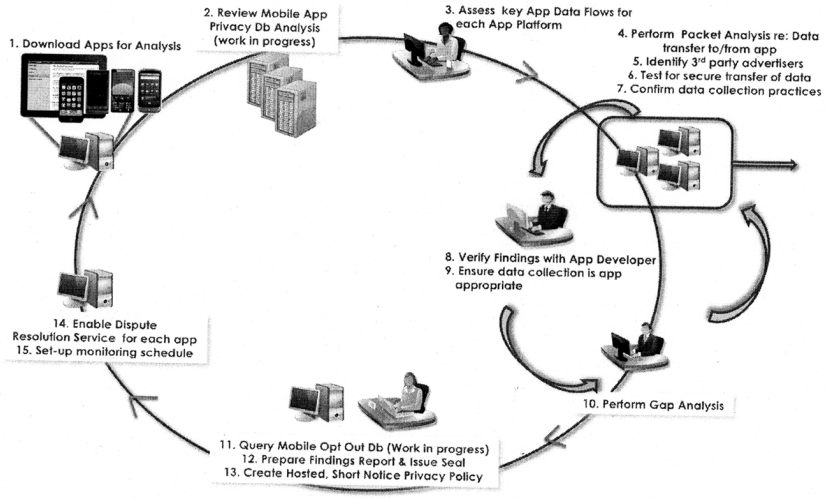
Most significantly, the TRUSTe—Harris survey demonstrates the extent to which privacy concerns continues to hamper consumer engagement on the mobile platform:

- 85 percent of the respondents restrict at least some type of information sharing on mobile applications;
- 40 percent of the respondents do not use sites that request personal information
- 38 percent of the respondents do not access their accounts via a mobile device
- 52 percent of the respondents are uncomfortable with the idea of signing in to other apps on their mobile device with another account ID (FB, Twitter), despite convenience
- 45 percent of the respondents would not share information about themselves with any company—even for a free or lower cost app
- More than 50 percent of the respondents would not be willing to share their location, address, date of birth on a smartphone; that number jumps to 92 percent when it comes to sharing a contacts list.

TRUSTe Analysis of Mobile Data Collection

TRUSTe also recently concluded an independent analysis of mobile data collection from the top 300 "free" apps on the Android, Apple and Blackberry mobile platforms. The goal of the analysis was to understand the type of data flows on the three most popular mobile platforms using a specific methodology that is part of our mobile certification process (Figure 4 below).

Figure 4. TRUSTe Mobile Labs—Mobile Privacy Certification Process



Our analysis yielded some interesting findings about mobile data collection practices. Analyzing the types of data collected by sample of the 300 most popular apps [13] on Android, Apple and Blackberry, we found that:

- Most apps (39 percent) collect geo-location data
- Most apps (39 percent) also collect data that allows the user to connect through their mobile device to Facebook, Amazon, Twitter, and other platforms.
- Only 23 percent of the apps had a privacy policy.

Conclusion

I want to reiterate TRUSTe's belief in self-regulation as the most effective way to address the privacy challenges posed by the mobile ecosystem. The mobile ecosystem is still in its very early stages; legislation or policy that is enacted in haste, or without careful thought, could easily freeze the robust innovation we currently see on the mobile web.

Self-regulation also provides us with the information needed to adapt a framework to evolving technologies. This is evidenced by our recent analysis and research on mobile privacy, conducted as part of our certification process. This research has given TRUSTe, our clients and sealholders, and our partners, important guidance for further product and market development.

In closing, I'd like to share some of these thoughts—specifically, what we think are the five essential requirements for a self-regulatory framework to be successful at protecting consumer privacy on the mobile web:

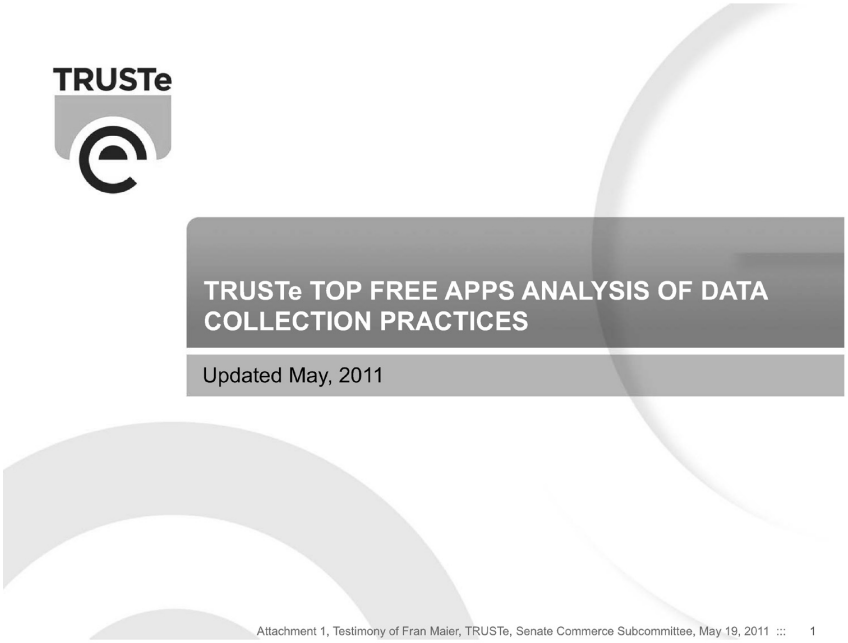
- First, TRUSTe believes that mobile apps and websites should have some form of *privacy policy* that informs the consumer about any collection and use of personal data. Our mobile privacy survey shows that a majority of consumers (74 percent) think it's important to know what type of data is being by their mobile apps. And, based on our sample of the top 300 most popular free apps, only 23 percent of apps have a privacy policy.
- Second, we think that consumers of mobile apps and websites should provide *choice for third party sharing.* This is especially true for geo-location and other types of sensitive data—consumers should give their express or opt-in consent for these types of data collection. Our survey showed for instance, that only 32 percent of smart phone users felt that they had a choice when it came to geo-location data collection.
- Third, *opt-outs should be provided for mobile advertising*—our survey showed that 85 percent of consumers want to be able to opt-in or out of targeted mobile ads. However, any choice mechanisms for online behavioral advertising and targeting should work across app directories and mobile platforms—otherwise, they won't be effective. We recognize that this is already a challenge due to the complex structure of the emerging mobile advertising industry and recommend that industry groups work together to develop consistent and workable approaches.
- Fourth, companies participating in a self-regulatory framework should abide by its requirements, and also *extend those requirements to relevant third parties,* such as application developers on their platform or service.
- Fifth, if legislation is contemplated, it should include a *safe harbor provision* and provide incentives for companies to join self-regulatory programs. Safe harbor provisions help foster the growth and promotion of best practices, which in turn is critical to the overall success of a self-regulatory framework.

I trust that the Subcommittee will find this testimony useful as it considers the important question of protecting consumer privacy in the mobile age. Thank you for your consideration.

---

[13] TRUSTe used the following sources to compile its list of the 300 most popular apps—Apple: *www.148apps.com*, Android: *101bestandroidapps.com* and *Androlib.com,* Blackberry: *Mobile.Blorge* and *HoneyTechBlog.com*.

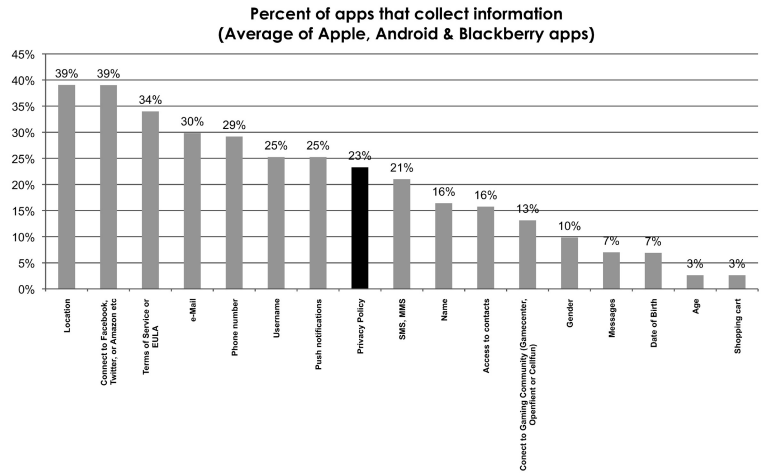
ATTACHMENT



- Goal: To understand the type of information collected by top free mobile apps on the three most popular platforms
  - Info that is most frequently collected
  - Range of information collected by apps
  - Key differences by platform re: info collected
- Source of Info: Top lists for free Apple, Android and Blackberry Apps as of January, 2011
- Date of updated analysis: May 16, 2010
- Methodology: Download, install and interact with the apps performing typical activities. Record type of information requested.

Top Apps List Source: Apple: www.148apps.com, Andoid: 101bestandroidapps.com and Androlib.com, Blackberry: Mobile.Blorge and HoneyTechBlog.com

Percent of Information Collected by Top 300 Free apps



N=300 (Apple:112, Android:153, Blackberry:35)