PATRICK J. LEAHY, VERMONT, CHAIRMAN

HERB KOHL, WISCONSIN
DIANNE FEINSTEIN, CALIFORNIA
CHARLES E. SCHUMER, NEW YORK
RICHARD J. DURBIN, ILLINOIS
SHELDON WHITEHOUSE, RHODE ISLAND
AMY KLOBUCHAR, MINNESOTA
AL FRANKEN, MINNESOTA
CHRISTOPHER A. COONS, DELAWARE
RICHARD BLUMENTHAL, CONNECTICUT

CHARLES E. GRASSLEY, IOWA
ORRIN G. HATCH, UTAH
JON KYL, ARIZONA
JEFF SESSIONS, ALABAMA
LINDSEY O. GRAHAM, SOUTH CAROLINA
JOHN CORNYN, TEXAS
MICHAEL S. LEE, UTAH
TOM COBURN, OKLAHOMA

BRUCE A. COHEN, *Chief Counsel and Staff Director*
KOLAN L. DAVIS, *Republican Chief Counsel and Staff Director*

United States Senate
COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510–6275

April 2, 2012

The Honorable Lawrence E. Strickling
Assistant Secretary for Communications and Information
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

Re: Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct (Docket No. 120214135-2135-01)

Dear Assistant Secretary Strickling:

I am writing to comment on the Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct. I agree with President Obama that our citizens' increasing willingness to share their personal information with others online does not suggest that privacy is an "outmoded value." I also agree with him that privacy has never been more important than it is today. The Internet is an incredible creation and more incredibly still, many of the best and most innovative sites and services on the web are available to users free of charge. Unfortunately, our privacy laws have not kept up with these changes and consumers are frequently and unknowingly paying for those innovations with their personal information and, inevitably, their privacy.

I submit these comments in my capacity as Chairman of the Senate Judiciary Subcommittee on Privacy, Technology and the Law. After a brief discussion of my own framework for thinking about privacy issues, I will focus my comments on two areas, responsive primarily to NTIA's first and fourth areas of comment.

First, I believe it is imperative that the Multistakeholder Process include and facilitate the participation of both strong consumer advocates and members of Congress. Second, I suggest three fields in which I believe that the Process could begin its work: (1) mobile privacy, specifically location privacy; (2) the privacy of biometric information, especially information derived from the use of facial recognition technology; and (3) the privacy of web browsing information and records. In each area, I lay out the substantive reasons for why further protections are necessary and then explain my own proposals for the standards that I believe are necessary to adequately protect privacy in these fields.

I. Privacy is a fundamental right.

Like most Americans my age, I grew up thinking of privacy as a right we hold against *government* intrusion into our lives. And to be sure, as law enforcement uses ever-more powerful technologies to track individuals and as the traditional constraints on law enforcement

activities—"limited police resources and community hostility"—are lowered, we must remain vigilant to government monitoring.[1] But as the recent result in the *Jones* case showed, while our Fourth Amendment jurisprudence may require updating, it still provides a baseline from which a Supreme Court as polarized as the current one may reach the right result for privacy.[2]

As I said in the first hearing of my Subcommittee, the Fourth Amendment does not apply to corporations. Outside of certain industries and market sectors, our privacy rights with respect to the private companies we interact with every day online are limited, if not entirely absent. Indeed, as I discuss further below, federal law allows your wireless company or smartphone company to disclose to non-governmental third parties a detailed record of everywhere you've been in the past month or year using geolocation data.[3] Similarly, there is no law that prevents a web browser from sharing your browsing history with its business partners, nor is there any law that prevents your social network from taking the photos you have posted online to share with your friends and using them to generate a precise and unique digital file for your face. I think that most Americans would be very surprised by this.

In light of the fact that much of commercial privacy law has yet to be written, I agree with President Obama that we need to return to "our timeless privacy values" and apply them to the new technologies and situations that we encounter in the 21st century. In my tenure as Chairman of the Senate Judiciary Subcommittee on Privacy, I have generally followed four principles in crafting legislation and performing oversight to protect our citizens' privacy.

First, I believe that all Americans have a fundamental right to *know* who has their personal information and how it is being used. This transparency principle is a critical privacy protection that is discrete from other consumer protection principles like consumer control and data security.

In November of last year, a security researcher discovered that smartphones from several major wireless carriers included monitoring software produced by a company called Carrier IQ that tracked various user activities on the phone, including users' locations and numerical keystroke data. When I learned of this, I immediately wrote Carrier IQ and the relevant wireless carriers to find out more.[4] My investigation revealed that the Carrier IQ software—combined with the way in which it was implemented on certain phones—in some instances transmitted the content of users' text messages and encrypted search terms to Carrier IQ, wireless companies,

---

[1] *See Illinois v. Lidster*, 540 U.S. 419, 426 (2004).

[2] *See United States v. Jones*, 132 S. Ct. 945 (2012) (Scalia, J., majority op.); *cf. United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (calling for a reconsideration of the third party doctrine, as it is "ill suited to the digital age").

[3] *See infra* Part III.

[4] *See* Letter from Senator Al Franken, United States Senator, to Larry Lenhart, Chief Executive Officer, CarrierIQ (Nov. 30, 2011), *available at* http://www.franken.senate.gov/files/letter/111201_Letter_to_CarrierIQ.pdf; Letter from Senator Al Franken, United States Senator, to Randall Stephenson, Chief Executive Officer, AT&T, and Dan Hesse, Chief Executive Officer, SprintNextel (Dec. 1, 2011), *available at* http://www.franken.senate.gov/files/letter/121101_Letter_to_ATT_HTC_Samsung_Sprint.pdf; Letter from Senator Al Franken, United States Senator, to Phillip Humm, Chief Executive Officer, T-Mobile USA, *available at* http://www.franken.senate.gov/files/letter/111206_Franken_Letter_T-Mobile_Motorola.pdf.

and other third parties.[5] But my investigation also revealed that the Carrier IQ software was a legitimate business tool used by several wireless companies to improve their users' experience and troubleshoot technical errors on smartphones. In fact, I think that these companies' greatest error was their use of this software in a manner in which the average consumer would have no idea that it was running on her device.[6] I suspect that most users would have readily consented to the use of this software on their phones if they had been presented with such a choice—ideally alongside a clear statement of how their data would be used and with whom it would be shared.

But transparency means more than simply burying disclosures in a privacy policy; transparency means making sure that users know about and understand how their data is being used. Countless studies have shown that consumers simply don't read privacy policies and that when they do, they have great difficulty understanding them.[7] Thus, I believe that when a company collects sensitive data or uses it in an unexpected manner, that company should at a bare minimum provide users *clear* and *salient* notice of the practice. For example, when OnStar used an inconspicuous terms and conditions update to inform its customers that it would reserve the right to collect their location information and share it with third parties *even after those customers had terminated their contracts*, I believe they violated this principle.[8]

Second, I believe that all Americans have a fundamental right to *control* who gets their personal information and who it is shared with. While I do not believe that a person who has voluntarily shared her data with a company has infinite downstream control over the subsequent recipients of that data, I do believe that she has the right to choose the third parties with whom the first party company can initially share her information. This is a well-established

---

[5] *See* Press Release, Senator Al Franken, *Sen. Franken Statement on Responses from Carrier IQ, Wireless Carriers, and Handset Manufacturers* (Dec. 15, 2011) (collecting responses from the letters), *available at* http://www.franken.senate.gov/?p=press_release&id=1891; Peter Eckersley, EFF.org, *Some Facts About Carrier IQ* (Dec. 13, 2011), *available at* https://www.eff.org/deeplinks/2011/12/carrier-iq-architecture; Jim Spencer, Minnesota Star Tribune, *Carrier IQ: Bug could've collected text messages* (Dec. 15, 2011), *available at* http://www.startribune.com/business/135708198.html.

[6] Trevor Eckhart, *Youtube Video: Carrier IQ Part #2* (Nov. 28, 2011), *available at* http://www.youtube.com/watch?feature=player_embedded&v=T17XQI_AYNo.

[7] *See, e.g.*, Yannis Bakos, Florencia Marotta-Wurlger & David R. Trossen, *Does Anyone Read the Fine Print? Testing a Law and Economics Approach to Standard Form Contracts*, New York University Law and Economics Working Papers Paper 195 (2009), *available at* http://lsr.nellco.org/nyu_lewp/195 (finding that only one or two website visitors per thousand will view the privacy policy and those visitors who do view it will not spend enough time reading to understand it); Joseph Turow et al., *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 I/S: A J. of Law & Pol'y for the Info. Soc'y 723, 740 (2007); N.Y. Times, *An Interview With David Vladeck of the F.T.C.* (Aug. 5, 2009), *available at* http://mediadecoder.blogs.nytimes.com/2009/08/05/an-interview-with-david-vladeck-of-the-ftc/. I found one statement of Mr. Vladeck's to be particularly telling: Mr. Vladeck, who directs the Bureau of Consumer Protection at the FTC and is charged with protecting consumer privacy, says "I'm a lawyer, I've been practicing law for 33 years. I can't figure out what the hell these consents mean anymore."

[8] I wrote a letter to OnStar asking that they rescind this change; they complied less than a week later. *See* Press Release, Senator Al Franken, *After Urging From Senators Franken and Coons, OnStar Reverses it's Privacy Policy* (Sep. 27, 2011), *available at* http://www.franken.senate.gov/?p=hot_topic&id=1760.

principle; it is what the Fair Information Practice Principles refer to as secondary external uses of information.[9]

I believe that this right is best illustrated by reference to the mobile apps on our phones. In December 2010, a *Wall Street Journal* investigation into 101 popular apps for iPhone and Android smartphones found that 47 of those apps transmitted the smartphone's location to third party companies, and that most of them did this without their users' consent. It is important to note that by virtue of the Android OS and iOS operating systems, the users of all but one of those 47 apps had expressly allowed the app itself to gather location information; they were unaware, however, that the apps were then disclosing that information to smartphone companies, analytics companies, marketers, and other third parties.[10] Thus, the users of these apps had no choice as to the secondary external uses of their location information. This is a serious violation of privacy.

Where the information being gathered is especially sensitive, the Individual Control principle should require more granular user choice over the sharing of information. For example, the Video Privacy Protection Act requires that video companies get their customers' permission every time they want to tell third parties what videos their customers watched.[11] As I explained in the third hearing of my Subcommittee, this is an important protection that allows a consumer to watch videos that relate to sensitive topics like religion, politics and sexuality without fear of inadvertently disclosing this information to family, friends, and co-workers. Privacy protections don't just protect our "right to be let alone": they also protect our right to liberty and our intellectual freedom.[12]

Third, I believe that our fundamental right to privacy includes the right to know that our sensitive information—wherever it is—is safe and secure. I am especially concerned that despite significant efforts to secure sensitive data, this right is still not being respected. Our treatment of sensitive health data is informative in this regard. Since the collection of breach records started in 2009, there have been a total of 409 major breaches of health data involving the health information of over 19 million Americans.[13] Note that this statistic only includes major breaches that have involved the health information of 500 or more individuals.[14] Note also that this comes nine years after implementation of the Health Insurance

---

[9] *See* Federal Trade Commission, *Privacy Online: A Report To Congress*, Part III.A.2 (1998), *available at* http://www.ftc.gov/reports/privacy3/fairinfo.shtm#Fair Information Practice Principles.

[10] *See* Scott Thurm & Yukari Iwatani Kane, Wall Street Journal, *Your Apps Are Watching You* (Dec. 17, 2010), *available at* http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html.

[11] 18 U.S.C. § 2710 (b)(2)(B).

[12] *See, e.g., Video and Library Privacy Protection Act of 1988: Joint Hearing on H.R. 4947 and S. 2361 Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the H. Comm. on the Judiciary and the Subcomm. on Technology and the Law of the S. Comm. on the Judiciary*, 100th Cong. 68 (1988) (written testimony of Janlori Goldman, Staff Attorney, American Civil Liberties Union) ("The danger here is that a watched society is a conformist society, in which individuals are chilled in their pursuit of ideas and their willingness to experiment with ideas outside of the mainstream."), *available at* http://www.loc.gov/law/find/hearings/pdf/00183854811.pdf.

[13] *See* U.S. Department of Health and Human Services, *Breaches Affecting 500 or More Individuals* (2012), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html (statistics accurate as of March 23, 2012).

[14] *See* 42 U.S.C. § 17932 (e)(4).

Portability and Accountability Act (HIPAA) Privacy Rule and three years after the passage of the Health Information Technology for Economic and Clinical Health Act (HITECH Act). I know for a fact that health providers around the country are working hard to secure this information. Unfortunately, this is not enough—and this illustrates that this may prove to be the most difficult of the privacy principles to successfully implement.

Fourth, I believe that concentration in the telecommunications and technology sectors has reduced the incentives for many companies to protect consumers' privacy. Consolidation in the telecommunications and technology markets has been happening at an alarming rate. This is particularly true in online markets, where many technology companies have focused their business models on the collection and aggregation of data. As a company obtains a dominant position in an online market, however, that company may have reduced incentives to protect consumers' privacy.[15]

But while *any* dominant company has lower incentives to meet consumer demands, the unique nature of the Internet economy may make these companies especially likely to act in a manner that is contrary to consumers' privacy. Many of the largest and most powerful Internet companies offer their products to consumers for free. Instead of requiring consumers to pay for their services, these companies "monetize" their activities by serving advertisements to those consumers—advertisements that are more effective and more lucrative if they are targeted to a consumer based on a detailed, individualized profile of that individual.[16] Internet companies are not just collecting consumer data by chance. Rather, an Internet company's financial success may turn in large part on its ability to beat its competitors in gathering data—ideally detailed, individualized data—about consumers.

We cannot rely on market forces alone to develop the best privacy policies for consumers. As companies collect and exploit consumer data, the Department of Justice (DOJ) and the Federal Trade Commission (FTC) need to recognize that these companies may have lower incentives to protect consumers' privacy, particularly if they have a dominant position in the market. As DOJ and the FTC review mergers and acquisitions, they should consider the potential implications for consumer privacy. DOJ and the FTC should also assess both whether consumers have an ability to choose another comparable product or service if they are unhappy with how their data is being treated, and also whether a company offers consumers choices, including the ability to opt-out of data collection or migrate their data to another service.

---

[15] Pamela Jones Harbour, a former Commissioner of the Federal Trade Commission (FTC) has noted that "[a]bsent pressure from competitors who might provide more attractive alternatives to privacy-prioritizing consumers, a dominant firm might rationally choose to innovate less vigorously around privacy or, perhaps to dole out privacy-protective technologies to the marketplace more slowly." Pamela Jones-Harbor & Tara Isa Koslov, *Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets*, 75 Antitrust L.J. 769, 795 (2010).

[16] *See* Pamela Jones-Harbor & Tara Isa Koslov, *Section 2 in a Web 2.0 World: An Expanded Vision of Relevant Product Markets*, 75 Antitrust L.J. 769, 780 (2010) ("In many Web 2.0 markets, the revenue stream is not matched directly to specific Internet-based services. Rather, to a large extent, revenue—or 'monetization," to use the current term of art—derives from the accumulation of data, which can then be put to myriad commercial uses."); *see also* Lori Andrews, New York Times, *Facebook Is Using You* (Feb. 4, 2012) ("[U]nlike other big-ticket corporations, [Facebook] doesn't have an inventory of widgets or gadgets, cars or phones. Facebook's inventory consists of personal data – yours and mine.").

Finally, I believe that federal and state authorities should rigorously enforce privacy laws—and that whenever possible, private citizens should have the right to personally enforce their right to privacy. Legislating and regulating to protect privacy is not enough. Even in the health care industry, where an increasingly established legal regime exists to protect health data, privacy violations appear to be going unaddressed. From passage of the Privacy Rule in 2003 through the end of 2010, the Department of Health and Human Services (HHS) received 24,275 health privacy complaints on matters it had the authority to investigate.[17] Of those, HHS has levied a formal fine, or Civil Monetary Penalty, in only one case and has reached monetary settlement agreements in six other cases.[18] To date, HHS has referred 499 cases to the Department of Justice (DOJ) for prosecution. In the second hearing of my Subcommittee, the Department of Justice told me that they had successfully prosecuted some of those 499 cases—but they could not tell me how many.[19]

Now, a large part of this apparent enforcement gap is due to HHS's wise policy of working cooperatively with businesses to fix privacy problems instead of resorting to prosecutions. And the apparent under-enforcement by DOJ could be due to the failure of Congress to impose more significant reporting requirements on that entity. But the message is clear—privacy problems are widespread in even the most sensitive sectors with established legal regimes, and all violators may not be held accountable by government.

Therefore, we can't rely solely on government enforcement: consumers also need to be able to hold companies accountable for violations. Privacy violations are difficult to detect, and when they are detected, the damage that consumers suffer is hard to quantify with a dollar amount. Both of these factors decrease the likelihood of government enforcement. For these reasons, I urge the NTIA to ensure that any implementations of the enforcement principle consider the role of enforcement by private citizens. I also urge the NTIA to take into account input from those who would be involved in such enforcement.

II. The multistakeholder process should include strong consumer advocates as well as input from Congress.

The NTIA has asked for input into which stakeholders should participate and what expertise those stakeholders should have. I believe it is essential that consumer advocates be fully considered in the multistakeholder process.

Business interests tend to speak out in greater quantity than consumer advocacy groups. When the Commerce Department requested comment on its report, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework" in December 2010, 66

---

[17] U.S. Dept. of Health and Human Services, *Historical Enforcement Data* (2012), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/historicalnumbers.html.

[18] U.S. Dept. of Health and Human Services, *Case Examples and Resolution Agreements* (2012), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html. At the time of the writing of this document, HHS was in the process of reaching a seventh monetary settlement agreement.

[19] *See Your Health and Your Privacy: Protecting Health Information in a Digital World: Hearing Before the Subcomm. on Privacy, Technology and the Law of the S. Comm. on the Judiciary*, 112th Cong. at 45:00 (Nov. 9, 2011), *available at* http://www.senate.gov/fplayers/jw57/commMP4Player.cfm?fn=judiciary110911&st=420.

companies and pro-business groups filed comment, while only 21 individual consumers and advocacy groups did so.[20] Business interests are also able to invest substantially more than consumer groups in making their voices heard in halls of power. In 2011, the 66 business advocacy groups who filed comment spent over $126,000,000 on total lobbying expenditures across all issue areas.[21] In contrast, the 21 consumers and advocacy groups who commented spent a mere $2,005,000 on total lobbying expenditures.[22] That is a substantial spending advantage for industry.

Because consumer interests are key to the multistakeholder process and what it aims to achieve, I urge the NTIA to require broad participation and consensus across *types* of participants, not just across *numbers* of participants.

Furthermore, because any effective proposal for a strong Consumer Privacy Bill of Rights will require legislation as well as self-regulation, members of Congress should also be involved in the multistakeholder process. Without the inclusion of legislators and their staffs, the multistakeholder process will fail to result in effective and enforceable protections for consumers.

III. The multistakeholder process should *comprehensively* address mobile privacy, particularly with respect to location information.

Beyond the issue of who participates in the multistakeholder process, the question of what issue to address is critically important. The NTIA Notice of Inquiry suggests that the application of President Obama's Transparency principle to mobile devices might be a suitable issue to address via the multistakeholder process. I would urge the NTIA to instead focus the multistakeholder process on the application of the entire Consumer Privacy Bill of Rights to the mobile environment, with a particular focus on sensitive information like location.

A. Location information is extremely sensitive, and yet we are not doing enough to protect it.

According to the CTIA, last year marked the first year in which the number of mobile devices in use exceeded the number of U.S. residents.[23] According to the Pew Internet Project, smartphones are now a majority of those mobile devices.[24]

---

[20] U.S. Dep't of Commerce, Notice of Inquiry, *Information Privacy and Innovation in the Internet Economy (Privacy and Innovation NOI)*, 75 Fed. Reg. 80042, Dec. 21, 2010, *available at* http://www.ntia.doc.gov/files/ntia/publications/fr_iptfprivacy_requestforcomments_12212010.pdf. All comments are available on the NTIA website at http://www.ntia.doc.gov/federal-register-notices/2010/information-privacy-and-innovation-internet-economy-notice.

[21] *See* Lobbying Database, OpenSecrets.org, http://www.opensecrets.org/lobby/index.php (last visited Mar. 20, 2012) (total expenditures were compiled by reviewing the profile of each commenter in this group, and adding each organization's "total lobbying expenditures" for calendar year 2011).

[22] *Id.*

[23] CTIA, *Semi-Annual Wireless Industry Survey* (June 2011), *available at* http://files.ctia.org/pdf/CTIA_Survey_MY_2011_Graphics.pdf.

Smartphones are rich sources of sensitive personal information: they contain not just the phone numbers and e-mail addresses of the people we communicate with, but also the contents of those communications. And because these devices are always with us—65% of people sleep next to their cellphones[25]—they also generate a precise, comprehensive record of our whereabouts. As Justice Sotomayor recently noted in the *Jones* opinion, these records can divulge "a wealth of detail about [a person's] familial, political, professional, religious, and sexual associations."[26] This information is extraordinarily sensitive and must be protected.

Unfortunately, this information is *not* being adequately protected and is being collected and shared with others, frequently without users' knowledge or consent. Even if we look only at location information, just one form of sensitive information generated by mobile devices, the number of abuses and breaches of this information is alarming:

- In January 2009, a special report by the Department of Justice revealed that approximately 26,000 persons are victims of GPS stalking annually, including by cellphone.[27]

- In December 2010, an investigation by the *Wall Street Journal* revealed that of 101 top smartphone apps, 47 disclosed a user's location to third parties without his or her consent.[28]

- In April 2011, consumers learned that their iPhone and Android smartphones were automatically sending Apple and Google information about the smartphone's whereabouts—even when users were not using location applications and, in Apple's case, even though users had no way to stop this collection.[29]

- In June 2011, Nissan Leaf drivers discovered that their cars automatically transmitted their vehicles' location, speed, and destination to many third party websites accessed through the car's computer.[30]

---

[24] Aaron Smith, Pew Internet and American Life Project, *46% of American adults are smartphone owners* (Mar. 1, 2012), *available at* http://www.comscore.com/Press_Events/Press_Releases/2012/3/comScore_Reports_January_2012_U.S._Mobile_Subscriber_Market_Share.

[25] *See* Amanda Lenhart, Pew Internet and American Life Project, *Adults, Cell Phones, and Texting* (Sep. 2, 2010), *available at* http://pewinternet.org/Reports/2010/Cell-Phones-and-American-Adults.aspx. This number is even higher for younger Americans—over 90% of Americans aged 18-29 sleep near their phones.

[26] *United States v. Jones*, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring).

[27] Katrina Baum, Shannan Catalano, Michael Rand, and Kristina Rose, *Stalking Victimization in the United States*, Bureau of Justice Statistics Special Report (January 2009), *available at* http://www.ncvc.org/src/AGP.Net/Components/DocumentViewer/Download.aspxnz?DocumentID=45862.

[28] *See* Scott Thurm & Yukari Iwatani Kane, *Your Apps Are Watching You*, The Wall Street Journal (December 17, 2010), *available at* http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html.

[29] *See* Julia Angwin & Jennifer Valentino-Devries, *Apple, Google Collect User Data*, The Wall Street Journal (April 21, 2011), *available at* http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html.

[30] *See* Darlene Storm, *Nissan Leaf secretly leaks driver location, speed to websites*, Computerworld (June 14, 2011), *available at* http://blogs.computerworld.com/18461/nissan_leaf_secretly_leaks_driver_location_speed_to_websites.

- In September 2011, users of smartphones running Windows Phone 7 software alleged (and subsequent research confirmed) that their phones transmitted users' precise coordinates back to Microsoft whenever the camera is switched on—even when users denied that app permission to access their location.[31]

- Later that month, OnStar informed its customers that it would continue to track their vehicles' speed and precise GPS locations "for any purpose, at any time" and reserved the right to sell that data to "any third party" provided that OnStar was satisfied that it would be safe to do so—*even if those customers had ended their OnStar service plans.*[32]

- In November 2011, consumers learned that some Android smartphones had pre-installed software that would automatically send a company called Carrier IQ a variety of information, including location—even though users had never heard of the software and had no way to turn off the data collection.[33]

Our federal laws do little to help the situation. Many people know that after *U.S. v. Jones*, the government has to get a warrant to track someone using a GPS device.[34] What most Americans don't know is this: Even after *Jones*, federal laws *allow* the companies that get location information from their customers' cellphones and smartphones every day to give that information to almost anyone they please—*without* their customers' consent. While the Cable Act and the Communications Act prohibit cable companies and phone companies offering telephone service from freely disclosing their customers' whereabouts, an obscure section of the Electronic Communications Privacy Act[35] allows smartphone companies, app companies, and even phone companies offering wireless Internet service to freely share their customers' location information with third parties without first obtaining their consent. The Department of Justice verified this in recent testimony before the Senate Judiciary Subcommittee on Privacy, Technology and the Law.[36]

---

[31] *See* Josh Halliday, *Microsoft sued for tracking mobile users' location without permission*, The Guardian (September 1, 2011), *available at* http://www.guardian.co.uk/technology/2011/sep/01/microsoft-location-tracking; Woody Leonhard, *Windows Phone 7 sends location data without your approval*, InfoWorld (September 26, 2011) *available at* http://www.infoworld.com/t/windows-phone/windows-phone-7-sends-location-data-without-your-approval-173986.

[32] *See* David Kravets, *OnStar Tracks Your Car Even When You Cancel Service*, Wired (September 20, 2011), *available at* http://www.wired.com/threatlevel/2011/09/onstar-tracks-you.

[33] *See* David Kravets, *Researcher's Video Shows Secret Software on Millions of Phones Logging Everything*, Wired (November 29, 2011), *available at* http://www.wired.com/threatlevel/2011/11/secret-software-logging-video/.

[34] *See United States v. Jones*, 132 S.Ct. 945 (2012). Of course, the Court left open the question of whether *Jones* applies to all forms of location tracking by law enforcement, though I believe that a warrant should be required for any tracking of the location of Americans, whether via physical GPS tracking device or by monitoring cell site location data.

[35] 18 U.S.C. § 2702(c)(6).

[36] Testimony of Jason Weinstein, Deputy Assistant Attorney General Criminal Division before the Senate Judiciary Committee (May 10, 2011), *available at* http://www.senate.gov/fplayers/CommPlayer/commFlashPlayer.cfm?fn=judiciary051011&st=2871.

B. The Location Privacy Protection Act is a solution to this problem.

I believe that my bill, the Location Privacy Protection Act,[37] provides a legislative solution to the privacy failures surrounding location information—and the law's current inability to protect that data.

The Location Privacy Protection Act (LPPA) would make sure that consumers have the ability to control their location information. Specifically, the LPPA would close current loopholes in federal law to require any company that may obtain a customer's location information from his or her smartphone or other mobile device to get that customer's express consent before collecting his or her location data and get that customer's express consent before sharing his or her location data with non-governmental third parties. The bill also contains a series of provisions to increase understanding and facilitate the investigation of stalking crimes that involve the misuse of location data. Finally, the LPPA creates focused criminal penalties for the worst abusers of location technology, including the knowing and intentional use of so-called "stalking apps" to facilitate violations of federal anti-stalking and domestic violence laws. My bill will both empower the average consumer and protect those individuals most vulnerable to the abuse of location technology.

The protections of the LPPA are squarely in line with President Obama's Consumer Privacy Bill of Rights. The Consumer Privacy Bill of Rights includes a principle of Transparency. Similarly, my location bill requires entities collecting or disclosing geolocation information to tell the person using the device: (1) what information will be collected and (2) who, specifically, it will be disclosed to, prior to disclosure. This information can't be buried within a privacy policy or terms of service. By requiring disclosure of this information in this way, consumers will be able to effectively access and understand information about who their information may be disclosed to.

The Consumer Privacy Bill of Rights includes a principle of Individual Control. To that end, my location bill requires entities to obtain express authorization prior to either collecting or disclosing consumer location information. Because location data is so sensitive, an express consent requirement is an appropriate way to implement individual control. At the same time, as I explained when I spoke on the floor of the Senate to introduce the legislation, my bill will *not* flood consumers with pop-up consent screens: a one-time consent screen will suffice.[38]

The Consumer Privacy Bill of Rights includes a principle of Respect for Context. By combining a requirement that entities inform consumers of both what location information will be collected and to whom it will be disclosed, prior to disclosure, with a requirement that entities obtain express consent to the collection and disclosure, contextual integrity is preserved. Consumers will be aware of how their information is being used and can ensure that it is used only within context.

---

[37] The Location Privacy Protection Act of 2011, S. 1223, 112th Cong. (2011).

[38] *See* 157 Cong. Rec. S3793-95 (2011), *available at* http://www.gpo.gov/fdsys/pkg/CREC-2011-06-15/pdf/CREC-2011-06-15.pdf.

Finally, the Consumer Privacy Bill of Rights includes a principle of Accountability. My bill provides enforcement by the Attorney General and by State Attorneys General. In the instance that neither the Attorney General nor any State Attorney General brings an action with respect to a specific breach, my bill also provides a private right of action to ensure that consumers can make sure that private companies adhere to their responsibilities under the LPPA.

As industry observers have noted, the Location Privacy Protection Act takes industry best practices and makes them the baseline for all actors.[39] And while it does not address all of the problems faced in the arena of mobile privacy, I believe that it shows the kind of success that legislative efforts can have if we reach out to every interested party from consumers to privacy advocates to industry. Location privacy isn't the only mobile privacy issue, however, and I think that the Location Privacy Protection Act could provide a useful model for developing future privacy standards for information like the contacts in our address books[40] and Universal Device Identifiers (UDIDs)—an identifier comparable to a serial number that every smartphone carries and that can be used to track all activity that occurs on a single phone.[41]

IV. The multistakeholder process should address biometric information privacy, especially with respect to facial recognition technology.

There is a variety of personal information that most people would consider private. Along with location information, I consider biometric information to be especially sensitive—and especially deserving of strong, explicit privacy protections. Biometric information is sensitive because it is *permanent*: unlike your credit card number, password, or even your home address, you can't change your face or your fingerprint. In some cases, it is also readily apparent and available for capture and analysis by anyone you come across on the street. And much like location information, this sensitive information is currently unprotected by our privacy laws.[42]

Because of this combination of sensitivity and lack of protection, I urge the NTIA to promptly address the issue of biometric privacy via the multistakeholder process. In particular, I urge the NTIA to examine information derived through the use of facial recognition technology.

---

[39] *See* Andrew Berg, Wireless Week, *Location, Privacy a Two-Lane Street* (June 27, 2011), *available at* http://www.wirelessweek.com/Articles/2011/06/Policy-and-Industry-Location-Privacy-Two-Lane-Street-Government/ (quoting Julian Sanchez, Research Fellow at the Cato Institute: "The effect of this legislation I think will be to effectively push app developers to do something that they were already supposed to be doing, and maybe some of them weren't.").

[40] *See, e.g.*, Daniel Terdiman, CNet, *Path shares photos--oh, and your contacts too* (Feb. 7, 2012), *available at* http://news.cnet.com/8301-13772_3-57372885-52/path-shares-photos-oh-and-uploads-your-contacts-too/.

[41] *See* Scott Thurm & Yukari Iwatane Kane, Wall Street Journal, *Your Apps Are Watching You* (Dec. 17, 2010), *available at* http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html; Kim-Mai Cutler, TechCrunch, *Amid Privacy Concerns, Apple Has Started Rejecting Apps That Access UDIDs* (Mar. 24, 2012), *available at* http://techcrunch.com/2012/03/24/apple-udids/.

[42] *See* Harley Geiger, Center for Democracy and Technology, *Seeing is ID'ing: Facial Recognition & Privacy* at 9 (Dec. 6, 2011), *available at* http://cdt.org/files/pdfs/Facial_Recognition_and_Privacy-CDT_Comments_to_FTC_Workshop.pdf ("Federal law does not explicitly address private sector use of facial recognition technology…"); Note, *In The Face of Danger: Facial Recognition and the Limits of Privacy Law*, 120 Harv. L. Rev. 1870, 1876-77 (2007) ("[E]xisting privacy law is simply ill-suited for this new invasion.").

A. In the already sensitive arena of biometrics, facial recognition is uniquely sensitive.

Facial recognition stands out within the world of biometrics for two reasons. First, unlike fingerprint identification, iris recognition, and several other biometrics, facial recognition technology can easily identify an individual in secret and at a distance—without that person having any idea that he or she has been identified.[43] Second, the raw data for facial recognition technology—faces—are associated with almost every aspect of our social and professional lives in a way that other biometric data are not. You put your photo, not your iris, on your LinkedIn profile and your social networking account. And when you leave your house, you only leave fingerprints on the things you touch; but unless you wear a mask, your face is captured by security cameras stationed on the streets you walk, the stores you visit, and the government buildings you enter.[44]

Your face can be the key to an incredible amount of information about you—and facial recognition technology can allow strangers to access that information without your knowledge, without your permission, and in about as much time as it takes to snap a photo. This is not hyperbole. Dr. Joseph Atick, Vice Chairman of the International Biometrics & Identification Association and a pioneer of facial recognition technology, put it this way:

> [A] person photographed by a mobile phone can be identified without their [*sic*] knowledge through face recognition using identity-tagged images harvested over the web. Add to this the powerful data mining capabilities provided by the ever-more sophisticated web search engines and we now have the ability to surreptitiously construct a detailed profile of someone we snap with our iPhone walking down the street.[45]

Indeed, researchers at Carnegie Mellon recently proved that they could use a consumer-grade digital camera, a collection of publicly available Facebook profile photos from Carnegie Mellon students, and off-the-shelf facial recognition from a company subsequently purchased by Google to successfully identify unknown students walking through a campus and correctly predict those students' interests and partial Social Security numbers.[46]

---

[43] In 2010, scientists at GE Global Research unveiled technology that would allow the recognition of an individual from a distance of 50 to 65 feet. *See* Frederick W. Wheeler et al., *Face Recognition at a Distance System for Surveillance Applications*, 2010 Fourth IEEE Conf. on Biometrics: Theory, Applications, and Systems, at 1. Even after the fact, snapshots and family photos can be used to create a faceprint without the pictured individual's permission.

[44] *See* Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* 46 (March 2012), *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf.

[45] Dr. Joseph J. Atick, *Face Recognition in the Era of the Cloud and Social Media: Is it Time to Hit the Panic Button?* at 3 (Oct. 2011), *available at* http://www.ibia.org/download/datasets/929/Atick%2012-7-2011.pdf.

[46] *See* Alessandro Acquisti, Ralph Gross & Fred Stutzman, *Faces of Facebook: Privacy in the Age of Augmented Reality* (Aug. 2011), *available at* http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/; Leena Rao, techCrunch, *Google Acquires Facial Recognition Software Company PittPatt* (Jul. 22, 2011), *available at* http://techcrunch.com/2011/07/22/google-acquires-facial-recognition-software-company-pittpatt/. For more detail regarding Dr. Acquisti's research, see Acquisti, Gross & Stutzman, *Faces of Facebook: Privacy in the Age of Augmented Reality Draft Slides* (Aug. 2011), *available at* http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/acquisti-faces-BLACKHAT-draft.pdf.

The government and private sector are not far behind. Right now, the Federal Bureau of Investigation is in the process of piloting a national facial recognition program for state and local police officers in Michigan, Washington, Florida, and North Carolina.[47] A range of commercial facial recognition apps are already available, and the latest operating systems for Android, iPhone and Windows smartphones include features that facilitate apps that use facial recognition technology.[48] Most recently, Hitachi announced a facial recognition system that can search through 36 million faces in one second, allowing it to recognize individuals walking in front of surveillance cameras in near real time.[49]

Once facial recognition technology is deployed pervasively, it could allow companies to prepare detailed profiles about consumers' shopping, traveling, and leisure habits without their knowledge or consent. But we need not wait for the future to see how the deployment of facial recognition technology, absent appropriate safeguards, raises significant privacy concerns.

Over the past 18 months, Facebook has rolled out a facial recognition feature known as "Tag Suggestions."[50] With an estimated 150 billion photos and an additional six billion more each month, Facebook has more photos than any company in the world.[51] What's more, with Facebook users tagging and identifying 100 million faces every day, Facebook has essentially crowd-sourced the large-scale, digital identification of the countless faces in those photos with unique names and identities.[52] Through the Tag Suggestions feature, Facebook leveraged its enormous database of tagged photographs and the ongoing tagging activities of Facebook users

---

[47] *See* Jesse Emspak, Discovery News, *FBI To Roll Out Face Recognition System* (Oct. 10, 2011) *available at* http://news.discovery.com/tech/fbi-face-recognition-system-111010.html.

[48] *See* Emily Steel, Wall Street Journal, *A Face Launches 1,000 Apps* (Aug. 5, 2011), *available at* http://online.wsj.com/article/SB10001424053111903885604576488273434534638.html; Robin Wauters, techCrunch, *Viewdle Releases SocialCamera for Android* (Apr. 27, 2011), *available at* http://techcrunch.com/2011/04/27/viewdle-releases-socialcamera-for-android-instant-photo-tagging-sharing/; Sarah Perez, techCrunch, *Bring On The Creepy! Faced.Me Is Building A New Facial Recognition App* (Nov. 23, 2011), *available at* http://techcrunch.com/2011/11/23/bring-on-the-creepy-faced-me-is-building-a-new-facial-recognition-mobile-app/; Ryan Paul, Ars Technica, *First Look: Android 4.0 SDK Opens Up Face Recognition APIs* (Oct. 21, 2011), *available at* http://arstechnica.com/gadgets/news/2011/10/first-look-android-40-sdk-opens-up-face-recognition-apis.ars; Mark Gurman, 9to5Mac, *Face detection software and API land in iOS 5 following Apple's 2010 purchase of Polar Rose* (Jul. 25, 2011), *available at* http://9to5mac.com/2011/07/25/face-detection-software-and-api-lands-in-ios-5-following-apples-2010-purchase-of-polar-rose/.

[49] Bryan Bishop, The Verge, *New surveillance system can compare your face against 36 million others in a single second* (Mar. 23, 2012), *available at* http://www.theverge.com/2012/3/23/2896525/new-surveillance-system-compare-your-face-against-36-million-others-in-one-second.

[50] *See* Justin Mitchell, Facebook, *Making Photo Tagging Easier* (original post Dec. 15, 2010, updated Jun. 30, 2011), *available at* http://blog.facebook.com/blog.php?post=467145887130.

[51] *See* 1000 Memories, *How Many Photos Have Ever Been Taken?* (Sep. 15, 2011), *available at* http://1000memories.com/blog/94-number-of-photos-ever-taken-digital-and-analog-in-shoebox; Mashable, *Facebook Infographic* (Oct. 21, 2011), *available at* http://mashable.com/2011/10/21/facebook-infographic/. This is not a close contest; by comparison Flickr has 6 billion photos and Library of Congress has approximately 15 million photographs and prints. *See* Flickr, *6,000,000,000* (Aug. 4, 2011), *available at* http://blog.flickr.net/en/2011/08/04/6000000000/; Library of Congress, *About PPOC* (last visited Dec. 22, 2011), *available at* http://www.loc.gov/pictures/about/.

[52] *See* Justin Mitchell, Facebook, *Making Photo Tagging Easier* (original post Dec. 15, 2010, updated Jun. 30, 2011), *available at* http://blog.facebook.com/blog.php?post=467145887130.

to create a massive database of its users' "faceprints"—unique digital files comparable to fingerprints that can be used to identify an individual based on his or her photograph. Because of the size of Facebook's photo collection and the speed with which its users are continuously tagging and identifying individuals in those photos, Facebook likely holds the largest and most accurate privately-held collection of faceprints in the world.[53] In fact, given that Facebook has 845 million users—and that the company opted all of its users into the program—a back of the envelope calculation suggests that Facebook could easily have a faceprint for one out of every twenty people on the planet.[54]

Facebook's roll-out of Tag Suggestions raised further concerns about Facebook's use of facial recognition technology. Facebook did not ask users to enroll in Tag Suggestions; rather, it automatically enrolled all of them in the program and then offered them a complex, multi-step process to get of it—and a separate, even more complex, multi-step process to delete the faceprints that Facebook had generated.[55] Moreover, the blog posts that Facebook used to announce Tag Suggestions do not make clear that the feature creates a unique, precise faceprint for each user tagged through Tag Suggestions.[56]

Tag Suggestions does in fact make it easier to tag your friends in photographs—a lot easier. And Facebook has since improved the ease with which consumers can opt-out of the program. These are good and helpful things. But because Tag Suggestions initially lacked basic, meaningful protections for users' personal information, Facebook's implementation of this feature has created tremendous privacy concerns.

I want to be clear: facial recognition technology could become a powerful and positive tool for public safety and private sector innovation. The key is to ensure that strong safeguards exist for privacy and civil liberties so that the benefits of these biometric technologies aren't outweighed by negative effects on privacy.

---

[53] *Cf.* Beth Wellington, The Guardian, *What Facebook Fails To Recognize* (Jun. 14, 2011), *available at* http://www.guardian.co.uk/commentisfree/cifamerica/2011/jun/14/facebook-facial-recognition-software (quoting leading cryptographer and computer security analyst Bruce Schneier: "Right now, Facebook has the largest collection of identified photos outside of governments. I don't think we know what the ramifications of that will be.").

[54] *See* Facebook, *Fact Sheet*, *available at* http://newsroom.fb.com/content/default.aspx?NewsAreaId=22; Population Reference Bureau, *2011 World Population Data Sheet*, *available at* http://www.prb.org/Publications/Datasheets/2011/world-population-data-sheet/data-sheet.aspx (identifying the world population at seven billion). My calculation assumes that 60 percent of Facebook users either opted-out of Tag Suggestions or had insufficient tagged photographs for the creation of a faceprint. I consider this to be a generous assumption. If only 20 percent of Facebook users opted-out or had too few tagged photos, Facebook could potentially have the faceprint of one out of every ten people on the planet. Despite requests from my Subcommittee staff, Facebook has declined to identify the number of faceprints it has created and currently holds.

[55] *See generally* Complaint, *In the Matter of Facebook, Inc. and the Facial Identification of Users* (Jun. 10, 2011), *available at* http://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf; Beth Wellington, *The Guardian, What Facebook Fails To Recognize* (Jun. 14, 2011), *available at* http://www.guardian.co.uk/commentisfree/cifamerica/2011/jun/14/facebook-facial-recognition-software; New York Times, *Facebook's 'Face Recognition' Feature Draws Privacy Scrutiny* (Jun. 8, 2011), *available at* http://www.nytimes.com/2011/06/09/technology/09facebook.html.

[56] Justin Mitchell, Facebook, *Making Photo Tagging Easier* (original post Dec. 15, 2010, updated Jun. 30, 2011), *available at* http://blog.facebook.com/blog.php?post=467145887130.

B. We can address privacy issues raised by facial recognition by applying the framework of the Consumer Privacy Bill of Rights

The multistakeholder process should address biometrics, with a focus on facial recognition technology, in order to put this technology on a path that will both promote innovation and protect the privacy and civil liberties of our citizens.

Dealing with facial recognition presents difficult challenges. As I mentioned above, you can capture someone's facial biometrics simply by taking his or her photo, and our photos are captured every day for a variety of important reasons, often without notice or an opportunity to express some kind of limitation on how that image—or the faceprint derived from it—can be used or disclosed. When Individual Control and Transparency are achievable, those principles must be followed; if a company *knows* it is gathering consumer photographs to convert them into faceprint files and create a digital database of faces, it should try to inform consumers of this before gathering their photographs and allow those consumers some degree of control over the generation of a faceprint unique to them. Likewise, those companies should inform consumers as to how faceprint data will be used and shared with others.

But given that the principles of Individual Control and Transparency may be difficult to achieve, a particular emphasis must be placed on other principles to preserve consumer privacy. In particular, entities that seek to use facial recognition information should abide by enhanced standards of Respect for Context, Security, and Focused Collection.

In order to abide by the principle of Respect for Context, entities collecting and disclosing facial recognition information must obtain that information in contexts that make it clear that the ultimate purpose of the collection involves biometric data analysis. It would be inappropriate for a photograph hosting service to convert faces in their photos to biometric data without providing consumer control over this function. It would be similarly inappropriate for a retail store to use its security cameras to identify the shopping patterns of a consumer and track that consumer across locations. In each circumstance, the context in which consumer photographic data is acquired is violated when the entity translates it into biometric data and uses that data to make comparisons.

Principles of Security and Focused Collection are similarly critical. Because this data is so sensitive, and especially because of its permanent nature, breaches of biometric data are particularly troubling. Where biometric data is necessary, strong security measures are equally necessary to minimize the risk of biometrics being misused, lost, or stolen. And biometric data is essentially permanent: my e-mail address or phone number might change every few years, but my faceprint will always be my faceprint. If biometric data is collected when collection is unnecessary, then more of this permanently relevant data will be stockpiled.

Unlike the problem of location privacy, I do not yet have a legislative proposal to address privacy and civil liberties issues surrounding facial recognition and biometric privacy. However, I believe that any solution to biometric privacy will require a combination of self-regulation and a legislative backstop to ensure that this uniquely and permanently sensitive information is not abused.

V. The multistakeholder process should address tracking of online activities.

Web browsing has become a significant part of Americans daily lives. From reading news to speaking with friends to watching movies, many of our most regular activities now occur online. As the Internet develops, this trend is likely to continue. A Forrester study from 2010 found that the average American spends 13 hours per week online, a 121 percent increase from five years prior.[57]

Unfortunately, various privacy breaches have revealed that consumer browsing data is not being protected in the manner it should be. And again, our laws do little, if anything, to protect this data. With the web involved in so many of our daily functions, it is essential that we have control over the privacy of our online activity.

A. Web browsing data provides a window into consumers' thoughts and interests. It is not being protected in the manner it should be.

The Internet provides virtually limitless information—and much of it can be sensitive in nature. Because of that, knowledge of an individual's browsing activities can be deeply revealing of personal information, such as health conditions, family crises, sexual orientation, and religious beliefs.

Just as Americans have expectations of privacy when they read a book at the library or rent a DVD to watch, they expect a reasonable level of privacy when visiting a blog or searching for clips on YouTube. I worry that those expectations are very far from reality; it appears to me that the tracking of online activities is pervasive and subject to little oversight.

For example, cookies—software that places an ID number on a computer so websites and advertisers can identify visitors—have been highly important to the success of the Internet. Online shopping, streaming video, and many other web functions are more effective and consumer friendly because cookies allow sites to have a consistent interaction with online users. However, cookies can also be used to track all online web browsing by individuals, threatening their privacy. Current law does not restrict companies' use of cookies or similar technologies to track web activities, nor does it restrict the sharing of this information with nongovernment sources.[58] In the absence of regulation, use of web tracking has been abused with increasing frequency. Here are just a few recent examples of these privacy breaches:

- In July 2011, *Wired* reported that KISSmetrics, an online tracking service used by popular websites such as Hulu and Spotify, was using techniques to track individuals online who had proactively taken steps to prevent such tracking. The service monitored and recorded online activities even if individuals had enabled private browsing and deleted their cookies.[59]

---

[57] Lauren Indvik, Mashable, *Americans Now Spend As Much Time Using Internet as TV [STATS]* (Dec. 13, 2010), *available at* http://mashable.com/2010/12/13/internet-tv-forrester/.

[58] *See In re DoubleClick Inc. Privacy Litigation*, 154 F.Supp.2d 497, 513 (S.D.N.Y. 2001).

[59] *See* Ryan Singel, Wired, *Researchers Expose Cunning Online Tracking Service That Can't Be Dodged* (July 29, 2011), *available at* http://m.wired.com/epicenter/2011/07/undeletable-cookie/.

- In September 2011, tech blogger Nik Cubrilovic discovered that Facebook was tracking users' web browsing even after they had logged out of their Facebook accounts.[60]

- In November 2011, it was revealed that Carrier IQ, a hidden smartphone application, was secretly recording a wide range of user activities, including web browsing and online searches.[61]

- In February 2012, the *Wall Street Journal* reported that Google had been circumventing privacy controls on Apple's Safari web browser to track individuals' activities online. This practice contradicted Google's own advice to users regarding web tracking, which previously stated that Safari's privacy settings would block tracking by the cookies Google was using.[62]

What is so disturbing about these incidents is that the web tracking was not only secret, but also occurred in circumstances in which individuals *had clear reason to believe* their web browsing was protected from tracking. When a user enables private browsing and deletes their cookies, they expect that this will stop web tracking. When a user logs out of an account, they believe that will stop that site from continuing to track them. If nothing else, when a company tells you "This is how you can avoid being tracked by our cookies," users should be able to assume that if they do what the company says, they won't be tracked by that company.

These instances of companies tracking users despite active attempts by users to prevent such tracking are not isolated events; these techniques are widely used online.[63] Rather, these events reflect an evolving system of web tracking that lacks transparency and proactively combats web users' attempts to protect their privacy.[64]

On February 23, 2012, the Digital Advertising Alliance (DAA) announced its members would support "Do Not Track" systems to give individuals control over web tracking.[65] I am pleased that the DAA and its members are engaging in efforts to protect consumer privacy

---

[60] *See* Dina ElBoghdady and Hayley Tsukayama, *Facebook tracking prompts calls for FTC investigation*, The Washington Post (September 29, 2011), *available at* http://www.washingtonpost.com/business/economy/facebook-tracking-prompts-calls-for-ftc-investigation/2011/09/29/gIQAVdsP8K_story.html; Nik Cubrilovic, New Web Order, *Logging out of Facebook is not enough* (Sep. 25, 2011), *available at* http://nikcub.appspot.com/posts/logging-out-of-facebook-is-not-enough.

[61] *See supra* Part III.A.

[62] *See* Julia Angwin & Jennifer Valentino-Devries, Wall Street Journal, *Google's iPhone Tracking* (Feb. 17, 2012), available at http://online.wsj.com/article_email/SB10001424052970204880404577225380456599176-lMyQjAxMTAyMDEwNjExNDYyWj.html#articleTabs%3Darticle.

[63] *See, e.g.*, Jonathan Mayer, Stanford Center for Internet and Society, *Safari Trackers* (Feb. 17, 2012), *available at* http://cyberlaw.stanford.edu/blog/2012/02/safari-trackers. Mayer notes that the Safari circumvention technique described above was widely used by a number of online ad networks.

[64] In describing the activities of KISSmetrics, privacy researcher and former FTC staff technologist Ashkan Soltani stated that, "These services are using practically every known method to *circumvent user attempts to protect their privacy*." (emphasis added). Ryan Singel, Wired, *Researchers Expose Cunning Online Tracking Service That Can't Be Dodged* (July 29, 2011), *available at* http://m.wired.com/epicenter/2011/07/undeletable-cookie/.

[65] Digital Advertising Alliance, *DAA Program Commended By US Regulators* (Feb. 23, 2012), *available at* http://www.aboutads.info/resource/download/DAA_Committment.pdf.

online. However, I believe this new policy contains several limitations which may make it insufficient to fully protect web users' privacy.

First, the DAA plan might not work with existing Do Not Track systems like those found in the Internet Explorer, Firefox, and Safari browsers. If DAA fails to work with the existing implementations of Do Not Track across these browsers, the DAA plan might make it more difficult for users to fully protect their privacy.[66] Additionally, it appears that the DAA may not respect browser settings that block tracking by default, instead requiring individuals to actively opt-in to a browser's Do Not Track system to prevent their activities from being monitored.[67] This will discourage browsers to enable Do Not Track by default, or lead to counterintuitive situations in which the browsers that are designed to be the most protective of privacy by default actually expose users to *higher* levels of tracking. Finally, current Do Not Track systems do not protect individuals who visit web pages through commonly used sources such as Google Search or Facebook so long as those users are currently logged into an account with those services.[68] Web sites with logged-in users will remain potentially able to track their users' activity across the Web, even after the implementation of Do Not Track.

I worry that tracking and documenting of web activities can potentially lead to disclosure of this private information, either voluntarily by those who collect it or through malicious action such as hacking. Further, I fear that the concern and lack of clarity regarding when individuals' browsing is being tracked could have a chilling effect, discouraging use of the Internet to communicate and learn.

B. What the Consumer Privacy Bill of Rights means for the protection of web browsing data.

These shortcomings reflect the need for the multistakeholder process to take further action to address the issue of web tracking. More generally, these flaws reflect that solutions to privacy problems require the input and support of consumers as well as business.

Achieving the White House's proposed principle of Transparency requires additional actions by both web browsers and entities that engage in tracking. Browsers should make clear what privacy settings are currently active, as well as the types of tracking that are generally permitted under each setting available. Entities that engage in tracking should inform users of what information is being obtained under their browser and current settings and ideally, whether or not that information will be shared with third parties.

Additional protections must also be put into place to achieve the principle of Individual Control with regard to web browsing. While browsers need not be required to make Do Not

---

[66] *See* Rainey Reitman, Electronic Frontier Foundation, *White House, Google, and Other Advertising Companies Commit to Supporting Do Not Track* (Feb. 23, 2012), *available at* https://www.eff.org/deeplinks/2012/02/white-house-google-and-other-advertising-companies-commit-supporting-do-not-track.

[67] *Id.*

[68] *See* Jeffrey Fox, Consumer Reports, *Two ways that Do Not Track won't protect your privacy* (Feb. 23, 2012), *available at* http://news.consumerreports.org/electronics/2012/02/two-ways-that-do-not-track-wont-protect-your-privacy.html.

Track their default setting, all browsers should contain a Do Not Track option that is clearly and conspicuously available to users.[69] All entities that engage in tracking should be obligated to fully respect Do Not Track systems, regardless of whether these systems are default settings. Further, the recent trend of developing new methods to circumvent privacy protections demonstrates that use of Do Not Track cannot be effective if it merely bars use of existing technologies and methods to track individuals online. Rather, a ban through Do Not Track must be comprehensive and prohibit *all* web tracking through any means, whether currently in existence or yet to be developed.

Respect for Context is also a critical principle when dealing with web tracking. The same search data that allows a search engine to adapt its results to a specific person's needs also allows that search engine to potentially provide an advertiser with a history of that person's search habits. Analytic data that a web retailer can use to improve its shopping interface can also be sold to marketers and used to market third party products to the user. Web sites must maintain a clear boundary between internal uses and external uses and make sure that where data could be used outside its original context, user transparency and control are enhanced.[70] Further, web sites should respect the principle of Focused Collection and avoid collecting information simply to collect information. While new uses for old data shouldn't always be avoided, data minimization and the removal of data after it is no longer needed help maintain consumer privacy by minimizing the possibility of data loss, theft, or misuse.

Finally, we must make sure that any Do Not Track system is enforceable and that entities that violate it can be held accountable. The FTC's recent announcement that it would use its enforcement authority against entities that promise to respect Do Not Track and fail to do so is a good start.[71] However, not every entity will promise to respect Do Not Track, and once data has been tracked by one entity, it can and will be sold to others.[72] Do Not Track and other methods of allowing users to exercise control over web tracking should be enforceable whether or not the tracking entity claims it will honor those privacy protections.

Significant progress has been made to protect the privacy of web users' online activities. However, the multistakeholder process must address concerns that persist, and create rules to empower all web users with the ability to fully protect themselves from online tracking.

---

[69] This would not be overly burdensome to web browsers. According to Christopher Soghoian, a Graduate Fellow at the Center for Applied Cybersecurity Research and former FTC staff technologist, "The technology behind implementing the Do Not Track header is trivially easy." Christopher Soghoian, slight paranoia, *The History of the Do Not Track Header* (January 21, 2011), *available at* http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html.

[70] *Cf.* Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* 40 (March 2012), *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf. The FTC's final report discusses how first-party marketing may generally require less consumer choice, but third-party and certain first-party practices will require more consumer control.

[71] *See* Federal Trade Commission, *FTC Issues Final Commission Report on Protecting Consumer Privacy* (Mar. 26, 2012), *available at* http://www.ftc.gov/opa/2012/03/privacyframework.shtm.

[72] *See* Julia Angwin, Wall Street Journal, *The Web's New Gold Mine: Your Secrets* (July 30, 2010), *available at* http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html ("[t]hese profiles of individuals, constantly refreshed, are bought and sold on stock-market-like exchanges that have sprung up in the past 18 months.")

VI. Conclusion.

I believe that privacy is a fundamental right—as fundamental as our freedom of speech or religion. I also believe that it is a right applicable not just against the government, but against the multitudes of companies and third parties that we encounter every day online and in the real world. My hope is that the multistakeholder process, combined with legislative action, will go a long way in making this right a reality.

Thank you for your consideration of these comments.

Sincerely,

AL FRANKEN
Chairman, Senate Judiciary Subcommittee
on Privacy, Technology and the Law