GEORGETOWN LAW

August 5, 2014

National Telecommunications & Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W., Room 4725
Attn: Privacy RFC 2014
Washington, D.C. 20230

VIA E-MAIL

Re: Comments of Alvaro Bedoya[1] & David Vladeck,[2] Center for Privacy & Technology at Georgetown Law, on "Big Data and Consumer Privacy in the Internet Economy," Docket No. 140514424-4424-01.

"Trust" is the first word of the President's Framework for Protecting Privacy. The Framework argues that consumer trust is necessary for the Internet economy to flourish, and that privacy is critical to maintaining that trust. It also argues that *individual control* – including control over the initial collection of data – is at the heart of that privacy mission.[3] We wholeheartedly endorse the Framework's focus on empowering consumers to make their own choices about sharing data.

We are concerned, however, that the Big Data Report[4] and the PCAST Report[5] shift the focus away from preserving trust by restoring control over personal data to consumers, to preventing *harm*, apparently on the theory that data collection is

[1] Executive Director, Center for Privacy & Technology, Georgetown University Law Center.

[2] Professor of Law & Faculty Director, Center for Privacy & Technology, Georgetown University Law Center. The views of the authors are provided in a personal capacity and do not necessarily reflect those of the Georgetown University Law Center or the Center for Privacy & Technology.

[3] The White House, CONSUMER DATA PRIVACY IN A NETWORKED WORLD (2012) at i ("Trust is essential to maintaining the social and economic benefits that networked technologies bring to the United States. […] Privacy protections are critical to maintaining consumer trust in networked technologies.").

[4] Executive Office of the President, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (2014)(hereinafter "Big Data Report").

[5] Executive Office of the President, President's Council of Advisors on Science and Technology, BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE (2014)(hereinafter "PCAST Report").

600 New Jersey Avenue, NW Washington, DC 20001-2075
PHONE 202-662-9000 FAX 202-662-9444

inevitable, regardless of consumer preferences. What's more, the Reports argue that *use limitations*, not individual controls over data collection, are the way to avoid harm.[6]

We agree with the Framework. A privacy framework must have as its foundation a commitment to the principle that individuals, not government and not corporations, ought to have control over the collection and use of personal data. We think that an approach to privacy protection that simply seeks to avoid "harm" is a poor one for many reasons. For one, it presupposes that individual control of data is impossible or undesirable, claims we reject. For another, "harm" is a poor benchmark for privacy because there is no consensus on what constitutes "harm," and every effort to define privacy harms has fallen short. To the extent that there is consensus about harm, it is simply that the concept does not capture the full range of privacy invasions that consumers suffer.

We also think that the right to individual control over data collection is crucial to privacy protection – and that use limitations, while an indispensable backstop, are a poor substitute for restoring to individuals the right to control the collection and use of their own data. In fact, we think that strong individual control over data collection may be necessary for *precisely* the vulnerable communities that the Big Data Report aims to protect.

I. Big data is not too big for consumer control.

The Big Data and PCAST Reports criticize the notice and consent model as outmoded. But they do much more than that: they argue that big data may be too big to control, *period*. "[A] sea of ubiquitous sensors, each of which has legitimate uses, make the notion of limiting information collection, challenging, if not impossible," the Big Data report says.[7] It cites Craig Mundie, who writes in *Foreign Affairs* that "simply so much data is being collected, in so many ways, that it is practically impossible to give people a meaningful way… to consent to its collection in the first place."[8] For them, ubiquitous data collection seems inevitable.

Ubiquitous, unconsented-to data collection is not inevitable, nor should it be. While data collection sometimes happens by accident, more often than not, it's the result of deliberate and often expensive engineering and policy decisions. In fact, the same

---

[6] *See* PCAST Report at 49-50 ("Policy attention should focus more on the actual uses of big data and less on its collection and analysis. By actual uses, we mean the specific events where something happens that can cause an adverse consequences or harm to an individual or class of individuals.").

[7] Big Data Report at 54.

[8] Craig Mundie, *Privacy Pragmatism: Focus on Data Use, Not Data Collection*, FOREIGN AFFAIRS, March/April 2014, *available at* http://www.foreignaffairs.com/articles/140741/craig-mundie/privacy-pragmatism.

technologies cited to support these arguments prove that it's quite possible to give consumers strong controls over their information in a supposedly big data environment.[9]

The Big Data Report says that "[f]acial recognition technologies can identify you in pictures online and as soon as you step outside."[10] That is true. Facial recognition technology is rapidly evolving. But it isn't automatic. It does not work by simply taking someone's photo. To be identified by a facial recognition system, an individual has to have his or her "faceprint" generated and enrolled into a facial recognition database. These databases operate in the United States today without any meaningful regulatory constraints.

That said, companies do not take the decision to create these databases lightly. After Facebook enrolled hundreds of millions of users into its facial recognition database without their permission, privacy regulators in Ireland and Hamburg forced the company to delete the faceprints of all E.U. citizens.[11] Google, on the other hand, has steadfastly maintained facial recognition as an opt-in offering on Google+ and has banned facial recognition apps from Google Glass.[12]

The Big Data Report also mentions the location tracking abilities of Wi-Fi technologies.[13] Again, while Wi-Fi-enabled devices automatically transmit MAC

---

[9] Here, it's worthwhile to recall Federal Trade Commission Chairwoman Ramirez's reminder that "Big data doesn't start as big data. Rather, it is assembled, bit-by-bit, from little data and becomes 'big' only when compiled into enormous databases." Chairwoman Edith Ramirez, Federal Trade Commission, *The Privacy Challenges of Big Data: A View from the Lifeguard's Chair*, Keynote Address, Technology Policy Institute, Aspen Forum, Aug. 19, 2013 (on file with the authors)(hereinafter "Chairwoman Ramirez") at 4.

[10] Big Data Report at 54.

[11] *See* Jessica Gyunn, *Facebook agrees to delete European users' facial recognition data*, L.A. TIMES, Sept. 21, 2012, *available at* http://articles.latimes.com/2012/sep/21/business /la-fi-tn-facebook-facial-recognition-europe20120921.

[12] *See* Clint Boulton, *Google's Opt-In Facial Recognition Avoids Facebook's Missteps*, EWEEK, Oct. 12, 2011, *available at* http://www.eweek.com/c/a/Security/Googles-Optin-Facial-Recognition-Avoids-Facebooks-Missteps-643462/; Google, *Glass Platform Developer Policies* (last updated July 9, 2014), *available at* https://developers.google.com/glass/policies. Granted, the proliferation of data-tagged images has made it possible for anyone to build their own facial recognition database. See Joseph Atick, *Face Recognition in the Era of the Cloud and Social Media: Is it Time to Hit the Panic Button?*, findBIOMETRICS, Oct. 19, 2011, *available at* http://findbiometrics.com/face-recognition-in-the-era-of-the-cloud-and-social-media-is-it-time-to-hit-the-panic-button-2/ (describing the "ease with which identification databases can be built from publicly available information in the cloud"). This is one of the many reasons that the NTIA is in the process of convening a Multistakeholder Process to set best practices for facial recognition technology. Currently, the leading pro-consumer proposal strongly endorses consumer controls on data collection. *See* ACLU, *An Ethical Framework for Facial Recognition* (last accessed on Aug. 5, 2014), *available at* http://www.ntia.doc.gov/files/ntia/ publications/aclu_an_ethical_framework_for_face_recognition.pdf. To the extent that the administration moves towards a focus on use limitations and away from collection controls, it undercuts any progress made by participants in a deliberative process that it has itself convened.

[13] *See* Big Data Report at 53.

addresses, commercial Wi-Fi location tracking services are far from automatic. A retailer seeking to track customers through their Wi-Fi addresses must purchase either stand-alone hardware or a wireless router that has been expressly pre-programmed for this functionality.[14] Moreover, while an industry has developed around non-consensual Wi-Fi-based location tracking in retail outlets, the second largest smartphone-maker, Apple, recently announced that its latest iOS8 operating system will block that technology in favor of opt-in systems.[15]

Ubiquitous collection does not "just happen." Some companies choose to collect data ubiquitously and without consumer consent. Others do not.[16]

II. Use limitations have their limits.

Use limitations are important. They are an essential backstop in a world where it is increasingly difficult for consumers to control the collection of their data. But we agree with Federal Trade Commission Chairwoman Edith Ramirez: "use restrictions have serious limitations and cannot, *by themselves*, provide effective privacy protection."[17]

Use limitations only work if you can identify, *ex ante*, the full range of potentially harmful uses for a set of data. Yet the PCAST Report suggests that this would be impossible, because "many sources of data contain latent information about individuals… that may become knowable only in the future with the development of new data-mining algorithms."[18] The Report seems to agree with Omer Tene and Jules Polonetsky, who write that "the possible uses of [big] data can be difficult to anticipate at the time of initial collection."[19] That observation is undoubtedly correct, but it makes our point: Use restrictions cannot address uses that are unheard of or unknown until the use takes place.

---

[14] *See* Euclid Analytics, *How it Works* (last accessed Aug. 5, 2014), *available at* http://euclidanalytics .com/product/how/.

[15] See Alex Hern, *Apple's iOS8 will stop retailers spying on customers via Wi-Fi,* THE GUARDIAN, June 10, 2014, *available at* http://www.theguardian.com/technology/2014/ jun/10/apples-ios-8-will-stop-retailers-spying-on-customers-via-wi-fi.

[16] *See also* David Vladeck, *Digital Marketing, Consumer Protection and the First Amendment: A Brief Reply to Ryan Calo*, 82 GEO. WASH. L. REV. ARGUENDO (2014)(forthcoming) at 5-7 (refuting the inevitability of ubiquitous tracking in the context of highly personalized digital marketing).

[17] Chairwoman Ramirez at 6 (emphasis added).

[18] PCAST Report at xi.

[19] *See* Omer Tene and Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STANFORD L. REV. ONLINE 63 (Feb. 2, 2012), *available at* http://www.stanfordlawreview.org/online/ privacy-paradox/big-data.

For use limitations to be effective, they also require that companies and consumers actually *agree* on which of those potentially harmful uses should be banned. In this sense, use limitations work well in a world where the interests of companies and consumers align, and there are a number of areas in which that is the case. But there are also many areas in which consumers' interests diverge significantly from those of the companies that serve them.

The divergence in interest may be the most pronounced for the poor, infirm, elderly, and racial or ethnic minorities. The research cited by the Big Data Report seems to acknowledge that: search engines treat first names associated whites and blacks differently;[20] online retailers quote higher prices to lower-income communities;[21] and data brokers create "sucker" lists of vulnerable individuals such as "X-tra Needy," "Ethnic Second-City Strugglers," and "Suffering Seniors," a list of elderly cancer or Alzheimer's patients.[22]

What the Big Data Report does not recognize, however, is that uses of data that seem acceptable to us today may be found entirely unacceptable later: harmful uses are often deemed harmful only after the fact. Society is especially slow to condemn – or even acknowledge – uses of data that hurt marginalized communities. For example:

- In 1942, Congress repealed the confidentiality protections of the Census,[23] letting the Census Bureau send block-by-block data on the locations of Japanese-Americans to the War Department. Many of them were subsequently rounded up and detained in internment camps.[24]

---

[20] *See* Latanya Sweeney, *Discrimination in Online Ad Delivery*, January 28, 2013, *available at* http://dataprivacylab.org/projects/onlineads/1071-1.pdf.

[21] *See* Jennifer Valentino-Devries, Jeremy Singer, Ashkan Soltani, *Websites Vary Prices, Deals Based on Users' Information*, WALL STREET JOURNAL, December 14, 2012, *available at* http://online.wsj.com/news/articles/SB10001424127887323777204578189391813881534.

[22] Senate Committee on Commerce, Science, and Transportation, A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES, MAJORITY STAFF REPORT, December 18, 2014, at 24. Charles Duhigg, *Bilking the Elderly, With a Corporate Assist*, N.Y. TIMES MAGAZINE, May 20, 2007, *available at* http://www.nytimes.com/2007/05/20/business/20tele.html?pagewanted=all&_r=0. *See generally* Federal Trade Commission, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014).

[23] Second War Powers Act, PUB. L. NO. 77-507, § 1402, 56 Stat. 186 (1942) (repealed). The measure passed the House on a near-unanimous voice vote. C.P. Trussell, *Wider War Powers Win Vote of House*, N.Y. TIMES, March 1, 1942.

[24] *See* Steven A. Holmes, *Report Says Census Bureau Helped Relocate Japanese*, N.Y. TIMES, March 17, 2000, *available at* http://www.nytimes.com/2000/03/17/us/report-says-census-bureau-helped-relocate-japanese.html (hereinafter "Holmes"); J.R. Minkel, *Confirmed: The U.S. Census Bureau Gave Up Names of Japanese Americans in WWII*, SCIENTIFIC AMERICAN, March 30, 2007, *available at* http://www.scientificamerican.com/article/confirmed-the-us-census-b/.

- In 1987, the U.S. Public Health Service instituted new mandatory AIDS tests for immigrants, subjecting 500,000 green card applicants to the blood tests annually and barring HIV-positive immigrants from permanent residence.[25]

- After World War II, the U.S. military engaged in wiretapping and mail surveillance to identify and dishonorably discharge gay servicemembers.[26]

Most of us now think that these cases of data use or collection were inappropriate, even repugnant. Yet the Census' role in the internment of Japanese Americans was only uncovered in the year 2000, after repeated denials by the Census Bureau.[27] The ban on gays in the military and the HIV travel ban were repealed *only in the last 5 years*.[28] Far too often, today's invidious discrimination was yesterday's national security or public health measure.

For these reasons, we believe that reliance on use limitations alone undermines any reasonable conception of privacy. If the right to privacy means anything, it is the right to say, as did Warren and Brandeis, "leave me alone."[29] The right to privacy has to

---

[25] Bernard Weintraub, *Health Officials Seek AIDS Tests for Immigrants*, May 16, 1987, N.Y. TIMES *available at* http://www.nytimes.com/1987/05/16/us/health-oficials-seek-aids-tests-for-immigrants.html.

[26] *See, e.g.*, Randy Shilts, CONDUCT UNBECOMING: GAYS AND LESBIANS IN THE U.S. MILITARY (2014) at 304.

[27] In 1983, a presidential commission concluded that the decisions surrounding the internment of Japanese-Americans were caused by "race prejudice, war hysteria and a failure of political leadership." REPORT OF THE COMMISSION ON WARTIME RELOCATION AND INTERNMENT OF CIVILIANS, PART 2: RECOMMENDATIONS (1983) at 5. Yet the role of the Census remained a secret until the year 2000 – 58 years after the fact. *See* Holmes at 17.

[28] President Obama ended the HIV ban in 2010, calling it "a decision rooted in fear rather than fact." By that time, the U.S. only one of a dozen countries that barred entry to the HIV-positive. *See* The White House, *Remarks by the President at Signing of the Ryan White HIV/AIDS Treatment Extension Act of 2009*, October 30, 2009, *available at* http://www.whitehouse.gov/the-press-office/remarks-president-signing-ryan-white-hivaids-treatment-extension-act-2009 (ending the ban effective January 2010). President Clinton announced "Don't Ask, Don't Tell" in 1993. Yet homosexuality investigations continued long afterwards. *See* Roberto Suro, *Navy Sends Agents into Gay Bars*, WASHINGTON POST, June 17, 2000, *available at* http://www.washingtonpost.com/wp-srv/WPcap/2000-06/17/045r-061700-idx.html; Tim Weiner, *Military Discharges of Homosexuals Soar*, N.Y. TIMES, April 7, 1998, *available at* http://www.nytimes.com/1998/04/07/us/military-discharges-of-homosexuals-soar.html.

[29] *See* Samuel Warren and Louis Brandeis, *The Right to Privacy*, 4 HARVARD L. REV. 5 (1890) at 193, 193.

give an individual a meaningful ability to prevent her data from getting into the hands others for uses that may serve the interests of the data collectors, but not the individual.

To be clear, this is not an argument against use restriction. Use limitations occupy an important place in a privacy protection regime. For example, strong, *ex ante* use limitations could have stopped Target from identifying pregnant women through their purchases.[30] Target would have of course collected the purchase data – the women would have still bought prenatal vitamins and maternity clothing – but a prohibition on medical profiling could have very much kept that genie in the bottle.

If someone truly wants to prevent the harmful use of his or her data, however, there is no better way to do that than to prevent its collection in the first place. As Chairwoman Ramirez has observed, "[i]nformation that is not collected in the first place can't be misused."[31]

The protection provided by individual controls is a necessity for groups that society has at some point deemed undesirable. The American public may never make up its mind about gay people, immigrants, minorities, and the poor – or how they and their data should be treated. Individual controls on data collection take that choice out of the hands of companies and the government, and into the hands of the individual.

Privacy is in many ways a shield for the weak. An *exclusive* focus on use limitations would take away that shield and replace it with promises.

III. Privacy law must aim higher than preventing harm.

Admittedly, this debate between individual controls and use limitations is something of a straw man. We expound on it here because, as noted above, the Big Data Report and the PCAST Report variously suggest that effective individual controls are impossible, and that a move away from individual controls and towards use limitations is not just inevitable, but strongly desirable. We must aim higher. It is perfectly possible to do both.

Nevertheless, while we think there may not be a need to choose between individual controls and use limitations, there *is* a clear choice to be made between the *goals* of privacy legislation as stated in the President's Framework for Protecting Privacy on the one hand, and the Big Data and PCAST Reports on the other.

---

[30] *See generally*, Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAGAZINE, Feb. 16, 2012, *available at* http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html? pagewanted=all.

[31] Chairwoman Ramirez at 6.

The PCAST Report argues that consumer privacy legislation should focus on preventing harms.[32] It says that this is what the public is worried about, too.[33] We do not think that the argument is persuasive. A review of some recent privacy controversies explains why.

In April 2009, iPhone users learned that their smartphones were silently recording their movements in an unencrypted file named "consolidated.db." The file was copied to any computer used to back up an iPhone. Users couldn't stop the logging. That said, the file was never sent to Apple or any third party. It could only be accessed through forensic software or a special, purpose-built app. And there was no evidence that it was misused – it actually helped mapping apps to run faster.

The response from users was nonetheless fierce. The controversy became known as "Locationgate." "Apple's locationgate scandal felt to many like a gross violation of privacy," wrote a *Wired* reporter. [34]

In November 2011, millions of Americans learned that their smartphones were sending a company named Carrier IQ location data, information on the apps they were using, and in some cases, the contents of their text messages. For most consumers, the app ran invisibly in the background; it couldn't be easily uninstalled.[35] The software was benign. In fact, it was a cutting-edge diagnostic tool used by many of the world's leading wireless carriers.

Yet consumers were outraged. Within weeks, Sprint announced that it was disabling the software on 26 million devices. Sprint was Carrier IQ's biggest customer.[36]

In April 2013, shoppers learned that certain retailers were monitoring their movements through their smartphones – without their permission, and in some cases, even when they didn't enter a store. The tracking could only be stopped through a

---

[32] PCAST Report at 49-50.

[33] *Ibid* at 5 ("Much of the public's concern is with the harm done by the use of personal data, both in isolation or in combination.").

[34] *See* Christina Bonnington, *Apple Pays Out $946 in 'Locationgate' Settlement*, WIRED, July 14, 2011, *available at* http://www.wired.com/2011/07/apple-locationgate-settlement/.

[35] *See* Zachary Lutz, *Carrier IQ: What it is, what it isn't, and what you need to know*, ENGADGET (last accessed Aug. 5, 2012), *available at* http://www.engadget.com/2011/12/01/carrier-iq-what-it-is-what-it-isnt-and-what-you-need-to/. *See generally* Carrier IQ, "Understanding Carrier IQ Technology," December 12, 2011.

[36] *See* Jaikumar Vijayan, *Sprint disables Carrier IQ software on its handsets*, COMPUTERWORLD, Dec. 16, 2012, *available at* http://www.computerworld.com/s/article/9222762/Sprint_disables_Carrier_IQ_software_on_its_handsets

complicated website opt-out. That is, if you knew where to find it: there was no requirement at the time that retailers even mention the location tracking to shoppers.

The company in question – Euclid – was no rogue. The company had done a lot of thinking about privacy and had strict use guidelines in place. The company scrambled – or hashed – the user data it collected and shared that data only in aggregated form.

Nevertheless, the following month, two of the company's most prominent clients – Nordstrom's and Home Depot – announced that they would drop the technology.[37]

In each of the above cases, the company was widely considered to have breached consumer privacy. Yet in each case, none of the consumers affected could point to a financial or physical harm. As Daniel Solove explains, these "visceral and vested" harms are generally the only kinds of privacy harm that American courts recognize.[38] Companies and courts may say "no harm, no foul." But when it comes to privacy, consumers do not buy it.

V. Conclusion.

We agree with the President's Framework. A consumer privacy bill should focus on preserving consumer trust by enacting into law the commands of the Privacy Bill of Rights. We ought not to settle on legislation that would do little more than protect against what the law currently defines as "harm."

This is not a new idea. It's an old one that dates to the birth of American privacy law and continues to this day. In 1890, Samuel Warren and Louis Brandeis wrote: "If privacy is once recognized as a right entitled to legal protection, the interposition of the courts cannot depend on the particular nature of the injuries resulting."[39] Scholars echo this belief today.[40]

---

[37] See Eli Epstein, *Nordstrom drops technology that tracks shoppers through smartphones*, MSN NEWS, May 10, 2013, available at http://news.msn.com/science-technology/nordstrom-drops-technology-that-tracks-shoppers-through-smartphones; Peter Cohan, *How Nordstrom's Uses Wi-Fi to Spy on Shoppers*, FORBES, May 9, 2013, *available at* http://www.forbes.com/sites/petercohan/2013/ 05/09/how-nordstrom-and-home-depot-use-wifi-to-spy-on-shoppers/ (citing Home Depot's discontinuation of Euclid's services).

[38] *See generally* Daniel Solove, *Privacy and Data Security Violations: What's the Harm?*, Linkedin, June 25, 21014, *available at* https://www.linkedin.com/today/post/article/ 20140625045136-2259773-privacy-and-data-security-violations-what-s-the-harm (explaining that "in most cases" courts do not recognize improper use, disclosure or sharing of data absent proof of "palpable physical injury or financial loss")(hereinafter "Solove").

[39] *See* Warren and Brandeis at 205.

[40] *See* Solove at 31 ("Although privacy/security violations cause harm, the legal system should move beyond its fixation with harm.").

The Administration should adhere to the recommendations in the President's Framework and move forward with legislation that effectively implements the Consumer Privacy Bill of Rights.