KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

COMMENTS TO NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION ON "BIG DATA AND CONSUMER PRIVACY IN THE INTERNET ECONOMY"

DOCKET NO. 140514424–4424–01

August 5, 2014

The Center for Democracy & Technology (CDT) is pleased to submit comments in response to the National Telecommunications and Information Administration's (NTIA) Request for Comments on "Big Data and Consumer Privacy in the Internet Economy", Docket No. 140514424–4424–01. We applaud the NTIA for continuing to examine the implications of "big data" upon consumer privacy, and look forward to working with NTIA and other government agencies on developing consumer-centric solutions in the big data context. Individual questions from the RFC, and CDT's response, are below.

I. Broad Questions Raised by the Big Data Report and the PCAST Report

1. How can the Consumer Privacy Bill of Rights, which is based on the Fair Information Practice Principles, support the innovations of big data while at the same time responding to its risks?

Consumer privacy legislation must empower individuals to make informed choices about how companies collect, use, share, and maintain their personal information. Today, it is very challenging for consumers to make privacy decisions — information about data practices is contained with dense, inscrutable privacy policies, often in such vague terms that not even an expert in the field could decipher them. As a result, consumers increasingly feel that their privacy is routinely violated by companies, and that they want more control over their information.[1] Privacy legislation should offer users that control. It should not, on the other hand, paternalistically assume that consumers cannot make reasonable decisions about their own privacy, or that the benefits of Big Data will always outweigh consumers' own subjective determinations of the value of their privacy and personal information.

Increasingly, we feel comfortable sharing sensitive personal information with companies that we rely upon for services. However, providing some information to a service provider should not imply that a user no longer possesses a privacy interest in that information. Gmail users feel comfortable sharing storing sensitive personal communications on Google's servers; that does not mean that they feel

[1] ONLINEPRIVACYDATA, Poll shows Americans deeply concerned about online privacy, mistrust social media, August 4, 2014, http://onlineprivacydata.com/release.html.

comfortable with *all* companies having access to that information for Big Data research. Similarly, cell phone customers collect sensitive geolocation information in providing voice and data services to users. That location information, however, is covered by CPNI rules,[2] and consumers reasonably do not expect information about their daily movements to be shared with the world (unless they themselves choose to publish that information). In short, increasingly sophisticated services mean that more companies have access to more information about us. But the knowledge of some by some certainly does not mean the knowledge of all by all.

In the government access context, the courts have increasingly recognized citizens' privacy interests in data that is nonetheless publicly observable or deliberately shared with third-party service providers. In *United States v. Jones*, for example, a majority of Supreme Court justices held that we have a privacy interest in our movements in public places, holding that a constant monitoring of a suspected drug dealer's car for a month violated a reasonable expectation of privacy and constituted a Fourth Amendment search.[3] In *Kyllo v. United States*, the Court held that even if marijuana cultivation could be detected by advanced technology from outside a residence, the use of that technology violated the resident's reasonable privacy interest.[4] .And most recently, in *United States v. Riley*, the Court implicitly questioned the third-party doctrine, noting that it might not even matter if data on a phone is locally stored on stored in the cloud, as the individual retains a reasonable privacy interest in that information.[5]

Similarly, commercial privacy law must recognize that merely because people are sharing more information with more companies, they still retain a privacy interest in how their data is collected, used, and retained. They also retain a privacy interest in the data they have not willingly shared, especially within traditionally private spaces such as their own homes. This privacy interest does not necessarily override all other considerations; however, it must be carefully weighed in determining how to provide information to consumers and how to set defaults for information collection and sharing. Wherever possible, however, consumers should be given the ability to control how their information is collected, used, shared, and retained.

---

[2] Testimony of Justin Brookman before the Senate Judiciary Committee Subcommittee on Privacy, Technology, and the Law, Hearing on "Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones, and Your Privacy," May 10, 2011, https://cdt.org/files/pdfs/20110510_mobile_privacy.pdf.

[3] *United States v. Jones*, 132 S. Ct. 945 (2012).

[4] *Kyllo v. United States*, 121 S. Ct. 2038 (2001). *See also Florida v. Jardines*, 133 S. Ct. 1409 (2013) (Kagan, J., concurring):

> A stranger comes to the front door of your home carrying super-high-powered binoculars. He doesn't knock or say hello. Instead, he stands on the porch and uses the binoculars to peer through your windows, into your home's furthest corners. ... Has your "visitor" trespassed on your property, exceeding the license you have granted to members of the public...? Yes, he has. And has he also invaded your "reasonable expectation of privacy"...? Yes, of course, he has done that too. That case is this case in every way that matters. (citations omitted).

[5] *Riley v. California*, 573 U.S. __ (2014).

2. Should any of the specific elements of the Consumer Privacy Bill of Rights to clarified or modified to accommodate the benefits of big data? Should any of those elements be modified to address the risks posed by big data?

We strongly believe that the White House's Consumer Privacy Bill of Rights should not be weakened in the name of Big Data. If anything, privacy protections and personal control should be strengthened — not eliminated — to allow consumers to make informed decisions about how to share their personal information in a world of ubiquitous sensors, indefinite storage, and powerful, opaque algorithms.

However, it is important to keep in mind that the White House's privacy report was written only two years ago, and it was drafted with the potential for (and pitfalls of) Big Data in mind. In the report's introduction, it states "[a]s abundance of data, inexpensive processing power, and increasingly sophisticated analytical techniques drive innovation in our increasingly networked society."[6] The report was carefully crafted to allow for societally beneficial use of personal information while still preserving privacy; notably, the word "innovation" occurs *54 times* in the report.

Specifically, the Respect for Context principle was developed to allow for beneficial secondary uses of data that are consistent with the purposes for which data was originally collected. Secondary use itself is hardly a new concept, but the 2012 White House report articulated a reasonable framework to legitimize secondary usage of personal information when that use is consistent with the context and rationale for the original collection. As the Big Data report rightly notes, this approach effectively endorses a "no surprises" rule that is consistent with user expectations and was roundly supported by international data protection commissioners at last year's data protection commissioners' conference in Warsaw, Poland.[7] Legislative language incorporating the Respect for Context principle should probably reference consumer expectations as a metric for evaluating whether a secondary use of information is consistent with the context in which the data was originally collected.

We would strongly reject any modifications to the Consumer Privacy Bill of Rights that do not provide for meaningful user control of personal information, limitations on data collection, or data minimization. *See infra*, pp. 4-7. Privacy law should not paternalistically presume that consumers will want all the benefits (and downsides) of Big Data at the expense of persistent monitoring of all of their behavior by any party. It simply cannot be the case that legislation should entitle everyone to learn all facts about everyone else, extinguishing the dignity afforded by personal privacy in the name of Big Data. Indeed, if the administration were to make any changes to its 2012 privacy framework, we would suggest that the provisions on data

[6] THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE DIGITAL ECONOMY 5 (2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[7] Privacy Commissioner's Office of New Zealand, Private Word Issue 86, *Information privacy commissioners target mobile apps*, December 2013, http://www.privacy.org.nz/news-and-publications/private-word/private-word-issue-86-december-2013/.

minimization be strengthened, and elevated to its own principle (data minimization is a standalone principle in many instantiations of the FIPPs).[8]

3. Should a responsible use framework, as articulated in Chapter 5 of the Big Data Report, be used to address some of the challenges posed by big data? If so, how might that framework be embraced within the Consumer Privacy Bill of Rights? Should it be? In what contexts would such a framework be most effective? Are there limits to the efficacy or appropriateness of a responsible use framework in some contexts? What added protections do usage limitation or rules against misuse provide to users?

While substantive limitations on data usage should play a role in any privacy protection framework, overreliance on reasonable commercial use requirements at the expense of individual autonomy and control would in most cases weaken — not strengthen — personal privacy protection.

Apart from any particular data usage, consumers have a clear privacy interest in controlling the collection of their personal information. As explained in our essay "Why Collection Matters,"[9] even static, unused data sets pose a considerable privacy risk — that data could be breached,[10] used maliciously by rogue actors within the company,[11] obtained by government without due process safeguards,[12] or later used in offensive ways by a company under earnings pressure.[13] Just as important, the fact of uncontrolled observation threatens trust, and may chill free expression and creativity.

Relying on responsible use will *always* be insufficient for a consumer's perspective — internal accountability mechanisms and privacy programs are a black box into which a consumer has no visibility. And indeed, in practice these mechanisms have proved insufficient. Many large, sophisticated companies have rigorous privacy programs with significant use limitations in place — and yet consumers have been susceptible to data breach, illegitimate government access, and deliberate actions that violated user privacy. As a result, there is a general sense among consumers that personal privacy is routinely violated, resulting in a lack of trust in the United States' privacy protection framework by American consumers[14] and foreign privacy regulators.[15]

---

[8] *E.g.,* Department of Homeland Security, Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security, Dece,ber 29, 2008, http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[9] Justin Brookman & G.S. Hans, *Why Collection Matters: Surveillance as a De Facto Privacy Harm*, FUTURE OF PRIVACY FORUM (2013), http://www.futureofprivacy.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf.

[10] *E.g.*, Consent Order, *In re DSW, Inc.*, File No. 052 3096, December 1, 2005 http://www.ftc.gov/sites/default/files/documents/cases/2005/12/051201agree0523096.pdf.

[11] *E.g..*, Consent Order, *In re Aaron's, Inc.*, File No. 1223264, October 22, 2013, http://www.ftc.gov/sites/default/files/documents/cases/131022aaronsagree.pdf.

[12] Theodoric Meyer, *No Warrant, No Problem: How the Government Can Get Your Digital Data*, PROPUBLICA, June 27, 2014, http://www.propublica.org/special/no-warrant-no-problem-how-the-government-can-still-get-your-digital-data.

[13] *E.g.*, Consent Order, *In re Gateway Learning*, File No. 042-3047, July 7, 2004, http://www.ftc.gov/sites/default/files/documents/cases/2004/07/040707agree0423047.pdf.

[14] ONLINEPRIVACYDATA, Poll shows Americans deeply concerned about online privacy, mistrust social media, August 4, 2014, http://onlineprivacydata.com/release.html.

Use limitations can do very little to alleviate concern about government access (or civil discovery), and incompletely protects against other threat models. Blanket reliance on responsible use naively presumes that institutions can perfectly control the data within their control — common experience shows that is not true.

Moreover, under a "responsible use framework," *which* institutions are to be trusted with the responsibility of using data in a responsible way? Will all data collection be presumed legitimate so long as certain proscribed data usages do not occur? Will all data transfers — indeed, all data publication — be legitimate? If that's the case, then *security is no longer a valid concern*; general access to all data is permissible because everyone is required to use that data responsibly. A moment's consideration reveals why this formulation is incredibly naïve. The fact of the matter is that not all institutions will use data responsibly because bad uses may be difficult to detect, or because criminals may be outside the scope of jurisdiction. Certainly, one would not feel comfortable posting one's Social Security and credit card numbers online with a mere caveat that anyone accessing that information has a binding legal obligation not to misuse it. Most existing privacy laws — ranging from peeping tom laws to the Wiretap Act — have substantive collection limitations that are not at all linked to an evaluation of how that data will be used. It would be a massive step backwards for privacy if those laws were revised to allow for persistent monitoring of private household activity or communications unless a harmful use could be demonstrated.

The traditional framework of control over data collection still makes sense: some information an individual's not going to have control over, for some data collection and usage there should only be an affirmative right to opt out from (such as, perhaps, online behavioral advertising or secondary data collection for analytics and research), and some sensitive information should only be collected with clear, opt-in consent. Our phones could record every action of our everyday lives and publish the results to the world (or just process the information in the cloud and keep it there indefinitely for one company's behalf) — excellent "Big Data" learning could happen from that, but few users would find the trade-off worthwhile. Rather, free expression and creatively would be massively curtailed under such a privacy framework.

Moreover, consumers and companies may not always share the same evaluation of what data uses are "responsible." Take for example the recent controversy about smart TV manufacturer LG: LG was revealed to be monitoring its customers' TV watching habits (as well as collecting file names from computers on the same network).[16] LG's actions were not necessarily *harmful* — the data collection was only designed to fuel a new LG behavioral ads product[17] — but the data collection by a television manufacturer (with whom customers traditionally don't have an ongoing data relationship after purchasing a TV) was clearly contrary to ordinary user expectations and many customers' preferences. The balance between the value of data and privacy should be determined by an individual — you cannot presume everyone is comfortable with all commercial data collection even for benign or beneficial uses, such as marketing and

---

[15] Paul Schwartz, *Differing Privacy Regimes: A Mini-Poll on Mutual EU-U.S. Distrust*, PRIVACY ASSOCIATION, July 22, 2014, https://privacyassociation.org/news/a/differing-privacy-regimes-a-mini-poll-on-mutual-eu-u-s-distrust/.

[16] Justin Brookman, *Eroding Trust: How New Smart TV Lacks Privacy by Design and Transparency,* PRIVACY ASSOCIATION, November 27, 2013, https://privacyassociation.org/news/a/eroding-trust-how-new-smart-tv-lacks-privacy-by-design-and-transparency/.

[17] LG SMART AD, http://us.lgsmartad.com/ (LG removed the video explaining its behavioral advertising product once consumers became aware of it).

research. Rather than paternalistically blessing all data collection as good for individuals unless harm can be shown, privacy legislation should empower users to make their own decisions about what sorts of services and data collection is beneficial for them.

That is not to say that consumers will be able to control all data collection in all scenarios. In public places, it is clear that some data about them will be collected (although retention limitations would help protect individual privacy interests in that data). Some products must collect certain data to work, and data may be maintained indefinitely (such as web-based e-mail). That does not mean, however, that *all* consumer products should be allowed to collect *all* potential personal information so long as they don't use that information for clearly harmful purposes.

Companies should have an obligation to make reasonable default determinations about what data will be collected, how that data will be used, how long that data will be retained, and even with whom the data will be shared. Based on the sensitivity of the data, the context in which it is collected, and the necessity of the processing, consumers should in many (if not most) cases have the ability to make decisions about how their personal information will be collected, used, and retained. Of course, if a company is not willing or able to honor a user's privacy preferences, it should not be obligated to provide that user with service. (*see infra*, p.17-18) (section on binding privacy controls).

4. What mechanisms should be used to address the practical limits to the "notice and consent" model noted in the Big Data Report? How can the Consumer Privacy Bill of Rights' "individual control" and "respect for context" principles be applied to big data? Should they be? How is the notice and consent model impacted by recent advanced concerning "just in time" notices?

Certainly, modern privacy policies have done a poor job of communicating data practices to consumers. Indeed, what we casually call "notice and consent" today is really neither — information provided to consumers in rote privacy notices is often unintelligible and incapable of being acted upon, and consumers certainly cannot reasonably be said to have mindfully consented to such data practices. However, merely because information and permission have not been successfully operationalized does not mean that they should not be done at all.

The Consumer Privacy Bill of Rights should distinguish between two related concepts: transparency (making information available about privacy practices) and notice (providing contextual information about privacy practices). On transparency, privacy legislation should include an affirmative requirement that companies actually explain data practices to consumers. Today, privacy policies are inscrutable, risk-averse compliance obligations, where the primary goal is often to avoid making an incorrect statement that could serve as a basis for FTC liability.[18] Thus, notices tend to be overly broad and vague.

While few consumers are likely to read even improved privacy policies, they would still play an important role. They would make actionable information available to those consumers who care enough to review, and regulators and consumer advocates who find certain practices objectionable could bring enforcement actions or call attention to bad practices. In short,

[18] Federal Trade Commission, What's the Deal? An FTC Study on Mobile Shopping Apps, August 2014, http://www.ftc.gov/system/files/documents/reports/whats-deal-federal-trade-commission-study-mobile-shopping-apps-august-2014/140801mobileshoppingapps.pdf.

improved transparency would force companies to be accountable for their actual practices, rather than let them fly under the radar, hoping that no one can evaluate what exactly they are doing.

In many cases, more prominent notice, delivered as close to the point of information sharing as possible, should be required to inform users about particularly surprising or sensitive data collections — prompting users to make an informed decision about whether to accept the offered terms or not. The FTC has already proposed guidance in how companies should approach modeling their notification systems. Specifically, they stated that companies should offer a choice not only at the most relevant moment but also within a context that is logical for the user.[19] Indeed, the FTC has recently pursued a number of cases under their existing Section 5 authority in which the FTC found that companies already have an affirmative obligation to convey practices (rather than merely reserving broad rights in privacy policies). For example, in their case against Goldenshores Technologies, which created one of the most popular apps for the Android mobile platform, the FTC argued that the company deceived its users by failing to disclose that the app transmitted the users' location (among other details) to third parties.[20] The settlement requires the company, "to provide a just-in-time disclosure that fully informs consumers when, how, and why their geolocation information is being collected, used and shared, and requires defendants to obtain consumers' affirmative express consent before doing so."[21]

We are also supportive of the notion of binding privacy preferences discussed in the Big Data and PCAST reports. Greater privacy threats require stronger, more comprehensive privacy controls that allow users to make universal decisions about the collection, use, transfer, and retention of their personal information. *See infra*, pp. 17-18.

5. Is there existing research or other sources that quantify or otherwise substantiate the privacy risks, and/or frequency of such risks, associated with big data? Do existing resources quantify or substantiate the privacy risks, and/or frequency of such risks, that arise in non-big data ("small data") contexts? How might future research best quantify or substantiate these privacy risks?

Privacy risks should not be defined only in terms of monetary or physical harm, but also must consider personal preferences and dignity of users, as well as the cost to free expression and adoption of technology from fear of privacy invasions. Some research has been done attempting to quantify risks of big data, but it has largely focused on costs to businesses or focused on specific professions (journalists, for example). This work has provided a good baseline for the value of privacy in an age of big data, but more work needs to be done on technical transparency and legal accountability.

---

[19] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," March 2012. p. 60, http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[20] Consent Order, *In re Goldenshores Technologies, LLC*, File No. 132 3087, December 5, 2013, http://www.ftc.gov/sites/default/files/documents/cases/131205goldenshoresorder.pdf.

[21] *Id.*; *see also* Consent Decree and Order for Civil Penalties, Permanent Injunction, and Other relief, *United States v. Path, Inc.*, February 1, 2013, http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathincdo.pdf.

Certainly, the revelation that commercial data is tied to government surveillance has fundamentally changed the conversation about big data. For the vast majority of consumers, unwanted surveillance — quite apart from practical effects of such surveillance — is the harm they're seeking to avoid. Therefore, considerations of risks associated with big data must address harms from government surveillance as well as private sector risks.

Researchers have attempted to quantify the harm of big data in monetary loses to businesses. The economic risks of big data can be observed in the losses to US technology companies as a result of US surveillance practices. Forrester Research estimated that the revelation of the PRISM program alone would result in, "a net loss for the service provider space of about $180 billion by 2016 which would be roughly a 25% decline in the overall IT services market by that final year."[22] These costs demonstrate the market value of business practices and government policies that respect privacy.

There are also quantifiable costs of data breaches to private industry. A study commissioned by IBM and conducted by the Ponemon Institute found that, "data breaches cost companies an average of $201 per compromised record – of which $134 pertains to indirect costs including abnormal turnover or churn of customers."[23] These estimates are useful, but fail to substantiate the effects on consumers rather than businesses. This is a particularly rich vein for research in light of the findings in the IBM study that showed that the largest increase in costs to companies with a data breach was a result of "increase in abnormal churn of existing customers by 15 percent."[24] It would be useful for future researchers to develop metrics that specifically address the economic risks for individuals in addition to businesses.

Additionally, there have been attempts to quantify the chilling effects on association and expression as a result of national surveillance. PEN America surveyed 528 of its members (writers, editors, translators, and agents) and found that 16% have, "Refrained from conducting Internet searches or visiting Web sites on topics that may be considered controversial or suspicious."[25] In another take on the same fundamental question, Human Rights Watch evaluated the effect of national surveillance programs on journalists by, "interviewing 46 journalists representing a wide range of news organizations."[26] The journalists reported an overall climate where they had difficulty contacting and security government sources and where they are moving more of their work offline to ensure security.

Small Data

The distinction between small data harm and big data harm is in some ways negligible in terms of risk to individuals. Small Data harms are often perpetrated by one individual against another, typically in a situation where the two have a pre-existing relationship or are in close proximity

---

[22] James Staten, "The Cost of PRISM Will Be Larger Than ITIF Projects," FORRESTER, August 14, 2013, http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects.

[23] IBM, 2014 Cost of Data Breach Study: United States. Ponemon Institute and IBM, p.5, http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/.

[24] *Id.* at p.6.

[25] PEN AMERICA, "Chilling Effects: NSA Surveillance Drives US Writers to Self-Censor," November 2013, p.6, http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf.

[26] HUMAN RIGHTS WATCH, "With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy," p.7 https://www.hrw.org/sites/default/files/reports/usnsa0714_ForUPload_0.pdf.

(physically or socially).[27] In both small and big data contexts, an individual's is always at risk of misuse when another possesses data about them. The consequences in small data breaches can be severe for individuals—a growing scholarship on revenge porn, for example, shows the huge emotional and financial costs of this type of small data harm.[28] However, the comprehensiveness, granularity, and unintuitive inferences possible in big data contexts magnify the implications of privacy risks in big data. For this reason, big data merits particular consideration.

Future Research
Scholars have presented compelling arguments that just the existence of large databases cause a threat to individuals, but this is difficult to quantify. Future researchers could play an important role in describing and quantifying the long-term risks of big data.

There are precedents for this kind of work in the analog world. For example, Danielle Citron compares databases of personal information to reservoirs of water collected to power saw mills in the Industrial Age. The stored water would sometimes leak, causing massive harm to the towns in the wake of the flood. Her analysis compares the policies that developed in response to that problem to the potential solutions for how to secure data in the Information Age.[29]

6. The Privacy Blueprint stated:

> *The Administration urges Congress to pass legislation adopting the Consumer Privacy Bill of Rights . . . Congress should act to protect consumers from violations of the rights defined in the Administration's proposed Consumer Privacy Bill of Rights. These rights provide clear protection for consumers and define rules of the road for the rapidly growing marketplace of personal data. The legislation should permit the FTC and State Attorneys General to enforce these rights directly . . . To provide greater legal certainty and to encourage the development and adoption of industry-specific codes of conduct, the Administration also supports legislation that authorizes the FTC to review codes of conduct and grant companies that commit to adhere — and do adhere — to such codes forbearance from enforcement of the legislation?*

How can potential legislation with respect to consumer privacy support the innovations of big data while responding to its risks?

No privacy protection framework can possibly allow for maximum usage of data while still completely safeguarding personal privacy; trade-offs will have to be made. We believe that these trade-offs should be evaluated and decided by the individuals whose information is affected — not by governments or corporations.

---

[27] Michael Birnhack, "S-M-L-XL Data: Big Data as a New I informational Privacy Paradigm," p.2.

[28] Danielle Keats Citron and Mary Anne Franks, Criminalizing Revenge Porn (May 19, 2014). Wake Forest Law Review, Vol. 49, 2014, p. 345+; U of Maryland Legal Studies Research Paper No. 2014-1, http://ssrn.com/abstract=2368946.

[29] Danielle Keats Citron, Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age. Southern California Law Review, Vol. 80, No. 2, pp. 241-297, 2007; U of Maryland Legal Studies Research Paper No. 2006-29, http://ssrn.com/abstract=928401.

As we have seen over the last ten years, a pure self-regulatory model for governing data privacy (bounded only by FTC Section 5 enforcement authority) has been widely recognized as insufficient to protect user's control of their personal information. On the other extreme, a legislative approach that prescribes detailed rules for each industry — including security standards and specific disclosure language — is unlikely to be flexible enough to adapt to new industries and business models, and may well discourage legitimate innovation that does not actually threaten consumer privacy.[30]

We believe that a principles-based legislation backed up by FTC, state attorneys general, and class action enforcement represents the most reasonable privacy protection framework, allowing privacy law to more quickly adopt to evolving technologies and businesses. The FTC's use of its existing unfairness authority to require reasonable security — one of the foundational Fair Information Practice Principles — has been extremely successful in targeting bad security practices and delineating rules of the road for other companies to follow.[31] After dozens of FTC security enforcement actions based on the principle of unfairness, it is fair to say that meaningful security for personal information is required by US law. However, that is not case for the other Fair Information Practice Principles.

We also support as part of privacy legislation allowing the FTC to endorse specific industry codes of conduct as compliant with privacy law, as a mechanism to provide adaptability and certainty to the privacy landscape. By giving the FTC the authority to certify certain practices as a statutory safe harbor from privacy enforcement, legislation would strongly incentivize industries to develop strong, rational codes that could be revised over time to adapt to new challenges. However, legislation should be quite clear that the FTC's approval authority, while given broad discretion, is still contingent upon a code addressing all elements of the Fair Information Practice Principles — including data collection limits, data minimization, and individual control. Industry codes must not be allowed to substitute commercial judgment for the users' own as to what is in their best interest.

II. Specific Questions Raised by the Big Data Report and the PCAST Report

7. The PCAST Report states that in some case "it is practically impossible" with any high degree of assurance for data holders to identify and delete "all the data about an individual" particularly in light of the distributed and redundant nature of data storage. Do such challenges pose privacy risks? How significant are the privacy risks, and how much such challenges be addressed? Are there particular policy or technical solutions that would be useful to consider? Would concepts of "reasonableness" be useful in addressing data deletion?

The difficulty in fully deleting all copies of data does pose privacy risks; however, it is simply incorrect to say that the limitations of data deletion mean that the value to imperfect deletion is nil. To the contrary, good faith yet potentially imperfect deletion still can play an essential role in protecting personal privacy. Moreover, in many organizations, there exist reasonable strategies

[30] Testimony of Leslie Harris before the House Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection, "The BEST PRACTICES Act of 2010 and Other Federal Privacy Legislation," July 22, 2010, http://democrats.energycommerce.house.gov/sites/default/files/documents/Testimony-Harris-CTCP-Best-Practices-2010-7-22.pdf.

[31] *Federal Trade Commission v. Wyndham Worldwide Corp.*, __ F.3d __, Civil Action No. 13-1887, slip op. (Apr. 7, 2014).

for periodically destroying hardware, such that there can be a reasonable level of confidence that at some point unneeded data sets are very likely to be eliminated from all servers.

Data is rarely if ever stored in a manner such that any data about an individual could be identified across an entire organization's information system and deleted. This means that some data, especially that which is stored in rarely-accessed or rarely-used data storage systems or backup systems, will endure for the storage life of those systems or data retention period set by organizational policy.

From a technical perspective, typical data deletion — for example what happens when a user empties the Trash or Recycling Bin on their computer's desktop — does not actually render the underlying data irretrievable, but only removes the data from the file list the computer keeps of active data in a filesystem. It is akin to reusing the paper in a filing cabinet, instead of shredding the paper or erasing the contents on the paper. To actually delete information on a digital storage medium (like a hard disk drive), a more complex process must be employed that writes over the existing data with random data to effectively destroy (or "shred") the deleted files contents. This means that many sets of deleted data may still be recovered off of discarded disk drives, and many common products, such as photocopiers,[32] contain disk drives and do not properly delete data that was temporarily stored on them.

For certain kinds of sensitive data, this disconnected data that remains in storage can be significant. Some sensitive data has a short shelf life for which the risks are fewer; for example, credit card information changes after 5-7 years, such that leaks of this information after this amount of time may not be relevant for common threats like financial identity theft. However, some types of sensitive data have much longer shelf lives, meaning the risks in these cases are much larger. For example, health information such as medical history, medication lists, and test results may allow someone to steal a patient's medical identity, or harm that individual for the rest of her life. A good data retention program that securely expunges data — physically destroying the storage medium or using media-specific secure erasure methods, such as degaussing for magnetic media — after the shortest time of utility would help ensure sensitive data does not exist indefinitely. Organizations that use data must remain vigilant against emerging sources of risk; e.g., if they learn that photocopiers may retain sensitive data, they will need to adapt their programs to cover these by employing secure destruction of the data and/or protection mechanisms provided by the manufacturer.[33]

However, the risk of potential recovery of deleted data does not mean that deletion is useless. Privacy protection should not let the perfect be the enemy of the good. Rather, a model that requires companies to exercise reasonable diligence to delete known copies of data, coupled with a commitment not to try to recover the data, still offers consumers significant protection against the threat models of data breach, subsequent misuse of data by the company, and illegitimate government access. Concomitantly, this reasonable degree of protection should lessen any chilling effect on consumer behavior created from concern over these threats.

---

[32] Armen Keteyian, *Digital Photocopiers Loaded with Secrets*, CBS NEWS, April 19, 2010, http://www.cbsnews.com/news/digital-photocopiers-loaded-with-secrets/

[33] For example, photocopiers by some manufacturers have security features that can provide a heightened level of protection. *See* KONICA MINOLTA, Application Solutions, http://participant.mykonicaminolta.com/content/products/subcategories/as_security.html

8. The Big Data Report notes that the data services sector is regulated with respect to certain uses of data, such that consumers receive notice of some decisions based on brokered data, access to the data, and the opportunity to correct or delete inaccurate data. The Big Data Report also notes that the other uses of data by data brokers "could have significant ramifications for targeted individuals." How significant are such risks? How could they be addressed in the context of the Consumer Privacy Bill of Rights? Should they be? Should potential privacy legislation impose similar obligations with respect to uses of data that are not currently regulated?

The risk of misuse of data by data brokers and others in the data services industry is non-trivial. As the recent FTC report on data brokers demonstrates, data brokers have a vast trove of data from a variety of sources.[34] As discussed above, massive databases can be ripe targets for unauthorized access or internal misuse without adequate security and oversight protections.

The FTC report also highlighted the lack of transparency in the current data broker ecosystem. As transparency is a core principle in the Consumer Privacy Bill of Rights, realizing the Bill of Rights would help protect consumers by bringing to light data broker practices. Because the data broker industry is somewhat obscure to most consumers, increased knowledge of what the industry does will help increase consumer trust and reduce the risk of misuse.

Because of the relatively recent history of discrimination based on data points like credit reports in the United States,[35] fears of "digital redlining" are far from speculative. These risks are significant given the ability to pinpoint individual consumers based on the data broker profiles and other records that could be used to create digital dossiers and categories that sort consumers based on categories such as race, gender, sexual orientation, or age. The Consumer Privacy Bill of Rights does suggest limitations on these kinds of uses, and CDT also supports the Civil Rights Principles for the Era of Big Data that were released this year.[36]

Ultimately, CDT supports consumer privacy legislation that increases oversight, gives consumers access to databases compiled about them, and provides for redress in order to avoid possible discriminatory applications or other types of tracking and classification antithetical to American values of privacy and equal opportunity. Today, consumers have little insight into the databases that companies compile about them, or into the algorithms that make determinations about them.[37] Consumers should have access to the former and more detailed information about the latter.

---

[34] Federal Trade Commission, Data Brokers: A Call for Transparency and Accountability, May 2014, http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[35] "The Color of Money: Home mortgage lending practices discriminate against blacks," ATLANTA JOURNAL-CONSTITUTION, May 1988, http://powerreporting.com/color/color_of_money.pdf.

[36] THE LEADERSHIP CONFERENCE, Civil Rights Principles for the Era of Big Data, http://www.civilrights.org/press/2014/civil-rights-principles-big-data.html.

[37] G.S. Hans, Are You a Two-Star Passenger? The Problem with Uber's Hidden Customer Rating System, CDT Blog, July 29, 2014 https://cdt.org/blog/are-you-a-two-star-passenger-the-problem-with-ubers-hidden-customer-rating-system/.

9. How significant are the privacy risks posed by unindexed data backups and other "latent information about individuals"? Do standard methods exist for determining whether data is sufficiently obfuscated and/or unavailable as to be irretrievable as a practical matter?

10. The PCAST Report notes that "data fusion occurs when data from different sources are brought into contract and new, often unexpected, phenomena emerge:" this process "frequently results in the identification of individual people," even when the underlying data sources were not linked to individuals' identities. How significant are the privacy risks associated with this? How should entities performing big data analysis implement individuals' requests to delete personal data when previously unassociated information becomes associated with an individual at a subsequent data? Do existing systems enable entities to log and act on deletion requests on an ongoing basis?

There are existing techniques that significantly limit the ability of an attacker to extract latent information from unindexed databases or to combine data across different sources. However, these techniques will not completely eliminate the possibility that latent data could one day be associated with an individual. Privacy legislation should incentivize database holders to continue to iterate on effective methods to obfuscate personal information while recognizing that complete confidence can never be achieved. Companies should act with knowledge of the potential for later unwanted data extraction, but should still undertake reasonable steps to prevent it.

As our response to question 7 alludes, the significance of privacy risks due to unindexed or latent data depends on the type of and sensitivity of the data involved. There are standard methods that can ensure data is sufficiently obfuscated or unlinked, but few other than physical destruction of storage media provide absolute assurance. Standard at-rest encryption mechanisms (either at the filesystem level or at the logical level using object encryption) provide a high degree of obfuscation and data protection. These techniques can render data practically erased at a much lower cost than logical or physical destruction if the keying material to decrypt the data is securely destroyed (encrypted data is practically indistinguishable from random data). However, encrypted sensitive data should eventually be securely written over or destroyed as efficient decryption or brute-force cracking techniques may will become practical in the future. Outside of encryption, techniques such as data sharding — where individual elements of a data record are distributed across widely geographically separated information systems — can ensure that the larger complete record is practically impossible to reassemble without access to each distinct information system in which the shards reside. These techniques must be implemented before data is stored, however. More ongoing, active means of assessing risk in latent information requires auditing data sinks and backups, including performing adversarial reidentification testing and risk analysis in order to determine the utility of data that hasn't be proactively treated.

The Supreme Court has repeatedly held that we retain a privacy interest in data that is observable or shared with service providers (*see supra*, p. 2); similarly, we retain a privacy interest in our information that resides in commercial databases even though we may not have complete confidence that that data can be deidentified or obfuscated. Consumers would certainly prefer that companies that wish to delete data actually try to do so, rather than concede defeat because it is not possible to do so with complete confidence.

11. As the PCAST Report explains, "it is increasingly easy to defeat [deidentification of personal data"] by the very techniques that are being developed for many legitimate applications of big data." However, de-identification may remain useful as an added safeguard in some contexts, especially when employed in combination with policy safeguards. How significant are the privacy risks posed by re-identification of deidentified data? How can deidentification be used to mitigate privacy risks in light of the analytical capabilities of big data? Can particular policy safeguards bolster the effectiveness of de-identification? Does the relative efficacy of de-identification depend on whether it is applied to public or private data sets? Can differential privacy mitigate risks in some cases? What steps could the government or private sector take to expand the capabilities and practical application of these techniques?

While there will always be a risk that deidentified data could potentially be reassociated with particular consumers, we believe that good faith, reasonable deidentification schemes represent a balanced approach to protecting personal privacy while still allowing commercial and scientific value to be extracted from data sets.

Certainly, data that is de-identified and intended to be distributed publicly poses a much higher risk towards re-identification than de-identified data that is distributed in a controlled, limited manner. The essential difference is that uncontrolled distribution allows for any other publicly available data set, or any private data set an attacker may have access to, to be brought to bear on the task of re-identifying records in the de-identified set. Accordingly, the risk of re-identification must be well worth the goals of releasing the data. Policy safeguards can go far, such as those outlined in the FTC Privacy Report, to the extent that they involve 1) enforceable public commitments to do de-identification well and to not allow re-identification. coupled with 2) contractually binding downstream recipients to not re-identify or further release de-identified data.

Anonymization of data — involving transforming the data via techniques such as aggregation, re/sub-sampling, noise injection, or record suppression[38] — is distinct from de-identification, and in many cases can be a superior method as long as granular detail in the data is not important for later analysis.

Differential privacy is a promising technique in theory, but it has seen little practical application. Differential privacy requires careful monitoring over time of queries made that might be dependent and leak more information in concert than each individual query may leak in isolation. However, some emerging techniques show promise, in this regard. For example, the model employed by the Patient-Centered Outcomes Research Institute[39] where the analysis is "brought to the data" and only aggregate statistics returned seems to offload some of the operational difficulties with managing privacy leakage budgets into human-based accounting and policy mechanisms.

The government and private sector need to invest more resources into both fundamental science associated with de-identification and privacy-preserving analytics, and also into

[38] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, April 10, 2014, http://www.cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf.

[39] PCORI, PCORnet: The National Patient-Centered Clinical Research Network, http://www.pcori.org/funding-opportunities/pcornet-national-patient-centered-clinical-research-network/.

practical implementation of these techniques that can be used in production software. For example, emerging techniques in matching between sets of data where the match can be performed without either side seeing the raw data of the other side are perfect for matching records between organizations without sharing the raw data or for matching records across an insecure boundary or transmission medium, like the Internet.[40]

12. The Big Data Report concludes that "big data technologies can cause societal harms beyond damages to privacy, such as discrimination against individuals and groups" and warns "big data could enable new forms of discrimination and predatory practices." The Report states that "it is the responsibility of government to ensure that transformative technologies are used fairly" and urges agencies to determine "how to protect citizens from new forms of discrimination that may be enabled by big data technologies." Should the Consumer Privacy Bill of Rights address the risk of discriminatory effects resulting from automated decision processes using personal data, and if so, how? How could consumer privacy legislation (either alone or in combination with anti-discrimination laws) make a useful contribution to addressing this concern? Should big data analytics be accompanied by assessments of the potential discriminatory impacts on protected classes?

As discussed above, the concerns regarding discriminatory uses of big data are very real given the relatively recent discrimination against minority groups based on data categorization. The Consumer Privacy Bill of Rights should be interpreted to bar such discriminatory uses of data, either through automated decisionmaking or through deliberate "digital redlining." Existing antidiscrimination law may, through rigorous enforcement, be sufficient to prevent these types of practices; however, consumer privacy legislation should make explicit a ban on discriminatory practices in order to eliminate any ambiguity.

Similarly, price discrimination — making assessments of a consumer's willingness to pay a certain price for a product or service based on other inferences — should be treated with skepticism. Markets function best when sellers offers their products at the price where they can generate a profit and outperform competitors. However, if Big Data simply exacerbates existing information imbalances between companies and consumers, consumers will be at a relative disadvantage, and may end up with less relative purchasing power than if prices were not set based on companies' estimates of what they are willing and able to pay. At the very least, companies must be transparent about the fact of price discrimination and the underlying data collection on which it is based.

Potential discriminatory impact assessments are a promising idea in order to prevent misuse of big data analytics; however, structuring such assessments and implementing oversight programs would require significant time and investment from the private sector. Moreover, without the voluntary release of such assessments and clarity regarding how companies audit their programs, it may difficult to ensure that they are being properly implemented and performed. Regulatory and co-regulatory oversight — as well as express commitments from companies — will in the short term likely be more effective in preventing big data analytics from being used for discriminatory ends.

[40] Michael Aaron, *Matching Without Sharing: Benefits and Challenges of a PSI Technique*, CDT, June 24, 2014, https://cdt.org/blog/matching-without-sharing-benefits-and-challenges-of-psi-technique/.

III. Possible Approaches to Big Data Suggested by the Reports and the Big Data Workshops

13. Can accountability mechanisms play a useful role in promoting socially beneficial uses of big data while safeguarding privacy? Should ethics boards, privacy advisory committees, consumer advisory boards, or Institutional Review Boards (IRBs) be consulted when practical limits frustrate transparency and individuals' control over their personal information? How can such entities be structured? How might they be useful in the commercial context? Can privacy impact assessments and third-party audits complement the work of such entities? What kinds of parameters would be valuable for different kinds of big data analytics to consider, and what kinds of incentives might be most effective in promoting their consideration?

Internal procedures for evaluating privacy procedures and risks are important and indeed necessary to preserve personal privacy. However, they are not sufficient, and invisible corporate procedures should not be substituted for individual self-determination and control over personal information.

Labeling internal privacy processes "accountability mechanisms" in some sense turns the original Fair Information Practice Principle of accountability on its head. Accountability as originally formulated meant that if a company violated one of the FIPPs, that company would be held accountable by external oversight (such as privacy regulators) for such violations.[41] However, by shifting privacy protection to opaque internal processes, consumers and regulators have less visibility into data practices, and fewer opportunities to hold institutions responsible for those practices.

Internal privacy programs are absolutely necessary for companies to make informed decisions about what information must be collected, how it will be used, how it will be shared, and how long it will be retained. Internal privacy programs also must consider what level of control to give users over their information, including default choices over whether certain information should be collected or used only with informed permission, collected and used with an opportunity for opt-out, or collected and used with no control at all. These decisions should be made based on a number of factors, including the sensitivity of the information, how the data will be used, and how related those purposes are contextually related to the purpose for which the consumer is using the service. However, the presence of internal privacy programs cannot be used to justify providing users with no insight into or control over data practices.

Already today, all leading Internet companies have extensive internal privacy programs; however, those programs have proven insufficient to protect user privacy, given consumer dissatisfaction with how their privacy is treated[42] and the ever-growing number of FTC privacy enforcement cases for violations of the United States's admittedly weak privacy laws.[43] Overreliance on internal mechanisms can further tilt the existing imbalance of power toward

---

[41] ROBERT GELLMAN, FAIR INFORMATION PRACTICES: A BASIC HISTORY (2014), http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.

[42] Katy Bachman, *Consumer Confidence in Online Privacy Hits 3-Year Low*, ADWEEK (Jan. 28, 2014, 10:04 AM), http://www.adweek.com/news/technology/consumer-confidence-online-privacy-hits-3-year-low-155255

[43] BUSINESS CENTER, BUREAU OF CONSUMER PROTECTION, LEGAL RESOURCES, http://www.business.ftc.gov/legal-resources/48/35 (last visited Aug. 5, 2014).

corporate decisionmakers and away from individuals. The Internet was built upon the democratizing power of empowering individuals via the end-to-end principle, privacy law should be used to justify entrenching decisionmaking and other power with large intermediaries and companies.

14. Would a system using "privacy preference profiles," as discussed in Section 4.5.1 of the PCAST Report, mitigate privacy risks regarding big data analysis?

15. Related to the concept of "privacy preference profiles," some have urged that privacy preferences could be attached to and travel with personal data (in the form of metadata), thereby enabling recipients of data to know how to handle such data. Could such an approach mitigate privacy risks regarding big data analysis?

We believe that legally sanctioned "privacy preference profiles" and metadata privacy rulesets are promising concepts, though these instructions should be configurable to extend to data collection and retention as well as simply use. In this way, for example, a consumer could tell a company that it feels comfortable sharing information with it, so long as the company agrees to delete or deidentify the data within six months. The company could then decide whether to offer the user the service under those terms.

This approach closely mirrors the work of the World Wide Web Consortium's Tracking Protection Working Group that CDT's Justin Brookman co-chairs, along with Matthias Schunter of Intel and Carl Cargill of Adobe. Under the Last Call Working Draft Technical Preference Expression specification,[44] users send a signal to websites that they don't want servers to collect, use, or retain information about that user's activity across different websites. A server can then respond that it complies with the signal and does no cross-service tracking at all;[45] that it disregards the signal and does not limit its tracking behavior;[46] that is has the user's specific consent to track despite the general no tracking instruction;[47] or that is limits its tracking to a specific set of conditions.[48] Based on this response, the user — or more likely, the user agent on behalf of the user — can make an informed decision about how to treat that transmission: it can allow it, block it entirely, limit the use of certain functionality (such as cookies or Javascript), or anything else it wants to do. Today, for example, EFF's Privacy Badger add-on[49] for Firefox and Chrome blocks third-party web requests to servers that don't adhere to their specified limitations on tracking data collection, retention, and use.[50]

There is no logical reason to limit these privacy preference profiles to data usage as envisioned in the PCAST report. While some may feel that there are no privacy interests raised by mere data collection and retention, others may disagree (perhaps for some of the reasons discussed

[44] W3C, Tracking Preference Expression (April 24, 2014), http://www.w3.org/TR/tracking-dnt/.

[45] *Id.* at § 6.2.4, http://www.w3.org/TR/tracking-dnt/#TSV-N.

[46] *Id. at* § 6.2.8, http://www.w3.org/TR/tracking-dnt/#TSV-D.

[47] *Id. at* § 6.2.6, http://www.w3.org/TR/tracking-dnt/#TSV-C.

[48] *Id.* at § 6.2.5, http://www.w3.org/TR/tracking-dnt/#TSV-T.

[49] ELECTRONIC FRONTIER FOUNDATION, PRIVACY BADGER, https://www.eff.org/privacybadger (last visited Aug. 5, 2014).

[50] ELECTRONIC FRONTIER FOUNDATION, A PRIVACY-FRIENDLY DNT POLICY, https://www.eff.org/dnt-policy (last visited Aug. 5, 2014).

here, see *supra* pp. 4-5, or perhaps for others). Legislation should not paternalistically make privacy decisions for consumers; rather, it should enable consumers to more effectively make their own privacy choices. If services demand access to certain information for at least some period of time, consumers can decide whether to accept those terms or not. In fact, users may very well cede control of their personal information in exchange for services. Let informed consumers and market dynamics work that out, rather than make the command decision that the inchoate benefits of Big Data to consumers will always justify the privacy costs.

16. Would the development of a framework for privacy risk management be an effective mechanism for addressing the challenges of big data?

As noted above, we strongly believe that risk management plays an important role in privacy protection. For this reason, we support the use of robust (but still potentially imperfect) deidentification schemes to allow for data transfer or publication while significantly minimizing privacy concerns.[51] However, because there is an inherent risk of misuse of any stored and identifiable data sets (*see supra*, pp.4-5), it is important to recognize that consumers have a privacy interest in *any* collection and retention of their personal information. This interest does not necessarily outweigh other interests or demand affirmative permission for each any every data collection and usage, but it is a consideration that institutions must keep in mind in considering how to protect personal privacy.

Properly understood, risk management must always play a role in determining how to limit the collection and misuse of personal information. On the other hand, risk management cannot simply be used as a rationalization for indiscriminate data collection unbounded by limits or controls. As the Article 29 Working Party recently stated, "the risk-based approach is being increasingly and wrongly presented as an alternative to well-established data protection rights and principles, rather than as a scalable and proportionate approach to compliance."[52] Risk management means that companies must consider all potential threat models to stored data, many of which are not addressed completely or at all by use limitations.

17. Can emerging privacy enhancing technologies mitigate privacy risks to individuals while preserving the benefits of robust aggregate data sets?

18. How can the approaches and issues in Questions 14-17 be accommodated within the Consumer Privacy Bill of Rights?

We are hopeful that privacy emerging technologies can develop that enable Big Data applications while minimizing the collection and storage of personally identifiable information. However, we do not believe that law should require the development of particular technologies; rather it should incentivize the development of and iteration of technological approaches to address clearly identified policy issues. Legislation should grant lesser protections to less identifiable data (including pseudonymous and deidentified data).[53] That differential treatment

[51] *See supra*, pp. 14-15.

[52] Data Protection Working Party, European Commission, Statement on the role of a risk-based approach in data protection legal framework (May 30, 2014), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

[53] CDT, CDT Analysis of the Proposed Data Protection Regulation, March 28, 2012, https://cdt.org/files/pdfs/CDT-DPR-analysis.pdf.

will encourage technologists to develop new approaches that can more reliably create less identifiable data sets or models that can take advantage of less identifiable data. If, on the other hand, such technologies cannot develop, companies and researchers will have to make consumers a value proposition for access to their data. If consumers see the value, they will use the service and provide their information. If they don't, their decisions should be respected.

Thank you again for the opportunity to provide feedback to your questions. If you have any follow-up questions, please contact us at 202.637.9800.

Justin Brookman
Director, Consumer Privacy

Joe Hall
Chief Technologist

G.S. Hans
Ron Plesser Fellow

Alethea Lange
Policy Analyst