Statement of Jules Polonetsky
Executive Director, Future of Privacy Forum

Testimony Before the California State Assembly Joint Committee
Hearing on Digital Privacy

Privacy Policies: Does Disclosure & Transparency Adequately Protect Consumers' Privacy?

Thank you for the opportunity to testify this morning. The Future of Privacy Forum (FPF) is a think tank seeking to advance responsible data practices and is supported by leaders in business, academia, and consumer advocacy.[1] FPF believes that the collection, analysis, and use of personal data provide many benefits both to consumers and society, and that innovative uses for data will only increase in the future. For the past four decades, the tension between data innovation and information privacy has been moderated by a set of principles broadly referred to as the Fair Information Practice Principles (FIPPs), but the FIPPs, particularly the principles of timely notice and choice, increasingly are under strain. New ways to protect consumers need to be explored.

I. *Notice Challenges and Opportunities: Privacy policies are not useful for many consumers, but are essential accountability mechanisms. Consumers need to be able to rely on the design and user interface of a service to quickly grasp how data is being used.*

Providing online notice is one of the few affirmative obligations that websites face.[2] Both California law and federally-recognized best practices require that companies providing online services link to a publicly-available privacy policy.[3] However, privacy policies frequently provide little help to consumers. According to one major study, online privacy policies have become so cumbersome that it would take the average person approximately 250 hours to read the privacy policies of every website he or she visits in a year.[4] Few people have the time to read privacy policies; fewer still have the time to understand what these policies even mean.

---

[1] FPF is led by internet privacy experts Jules Polonetsky and Christopher Wolf. The views herein do not necessarily reflect those of the Advisory Board or supporters of the Future of Privacy Forum.

[2] M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1028 (2012).

[3] *Id.* (citing CAL. BUS. & PROF. CODE §§ 22575–22577 (West 2008)).

[4] Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY (2008 Privacy Year in Review issue), *available at* http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.

Furthermore, studies have shown that "[w]hen consumers see the term 'privacy policy,' they believe that their personal information will be protected in specific ways; in particular, they assume that a website that advertises a privacy policy will not share their personal information."[5] In reality, however, the existence of a privacy policy is not a guarantee of privacy. Among practitioners in the field, it is common knowledge that privacy policies serve more as liability disclaimers for businesses regarding their use of personal data rather than assurances of privacy for consumers.

However, privacy policies set the boundaries for data use by businesses beyond those that might be prescribed by law. While businesses often use privacy policies to articulate and enable broad use of data for various purposes, the privacy statements often set boundaries on permissible use by the business.

Thus, privacy policies are critically necessary. The principal value of privacy policies is that they provide accountability to regulators and privacy experts who are in a better position to meaningfully review corporate privacy policies. Additionally, disclosure requirements by themselves can force companies to evaluate their privacy practices and instill discipline in how they treat consumer information.[6] Privacy policies do have great value as a disclosure mechanism and as an accountability mechanism. And by making privacy policy statements a company creates legal obligations that are enforceable by State Attorneys General and the Federal Trade Commission.

Notwithstanding the utility of privacy policies for regulatory and accountability purposes, we need to think creatively about how to provide consumers with meaningful insight into corporate data practices. Increasing transparency is one solution, but transparency does not simply mean better privacy policies. Instead, policymakers should encourage companies to engage with consumers in a meaningful conversation where both parties' interests and expectations can be aligned.[7] Companies can frame relationships by "setting the tone" for new products or novel uses of information. The lesson for companies is that context is key. For unexpected new uses of data, users should be brought along carefully, educated and, when appropriate, given an opportunity to object. Even where new uses of data are contextually similar to existing uses, information and education are key. Amazon serves as a prime example of this approach: its website is able to pursue a high degree of customization without violating consumer expectations, given its clear messaging about customization and its provision of a user interface frames how data is used.

Most consumers get their information about the collection and use of their personal data not from privacy policies, but rather from how user interfaces work and the basic information and cues they see as they use a service. Techniques to inform consumers of data practices might include symbols, short phrases, colors, diagrams, or any of the tools otherwise available to designers seeking to provide users with an engaging user experience. Engaging consumers about data use should be viewed as an essential feature and a core part of the user experience. In the end, design features that "communicate" information to users may be more helpful than traditional notice models.

---

[5] Joseph Turow et al., *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3(3) I/S: J. L. & POL'Y FOR INFO. SOC'Y 723, 724 (2007).

[6] *See* Peter P. Swire, *The Surprising Virtues of the New Financial Privacy Law*, 86 MINN. L. REV. 1263, 1314 (2002).

[7] *See, e.g.*, Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms* (forthcoming YALE J. OF L. & TECH., 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2326830.

II. *Disclosure Requirements: Legislating disclosure requirements for rapidly changing technology or when standards are still evolving is not effective.*

Even as regulators continue to view notice as the most fundamental of the FIPPs, there remains uncertainty over what information matters for disclosure.

What do we mean by disclosure? Should companies be required to provide information about the privacy controls of every internal technical mechanism or outside vendor? The European Commission has recently called for American companies operating under the U.S.-EU Safe Harbor to "publish privacy conditions of any contracts they conclude with subcontractors" such as cloud service providers.[8] The inclusion of those provisions would only lengthen and complicate privacy policies.

How should companies disclose information about data collection and data use? California has waded into the Do Not Track (DNT) debate with its recent amendment to the California Online Privacy Protection Act (CalOPPA), which now requires websites to disclose how they respond to a DNT signal or too provide a link to an industry self-regulatory program that provides tracking controls.

There is much ambiguity over what DNT means, and most companies are awaiting consensus from the World Wide Web Consortium (W3C) before attempting to implement DNT. Less than a dozen have publically committed to responding to a DNT signal. As a result, most web sites will need to comply with California's new law by amending their privacy policies to state that they do not currently respond to DNT signals but may do so in the future.[9] But many other web sites, including the companies that do most of the more sophisticated tracking, may rely on a provision of the law to say nothing new because they are already involved in industry programs. And sites that do track, but don't use personal information as defined by the new law, can also ignore the new requirements. Industry is confused and consumers - if they pay attention – will be completely befuddled.

FPF has launched a consumer focused web site at www.allaboutdnt.org to try to clearly explain tracking options to consumers and we are encouraging companies to point consumers to it. And although we hope the site is useful, we aren't convinced that many consumers would want to wade through the dozens of pages of information we have provided at every web site privacy policy they encounter. We appreciate the intention of the legislature in wanting to encourage efforts to advance a Do Not Track setting for consumers that is meaningful, but we need ways for legislators to use the bully pulpit to encourage progress rather than legislation when a standard is a moving target.

Regulators and policymakers should pursue a more coherent approach that can more flexibly encourage companies to provide what consumers need to know .[10]

---

[8] *Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*, at 19, COM(2013) 847 (Nov. 27, 2013), *available at* http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf.

[9] Bret Cohen, *New California Law to Require Additional Web Privacy Policy Disclosures*, HOGAN LOVELLS CHRONICLE OF DATA PROTECTION (Sept. 9, 2013), http://www.hldataprotection.com/2013/09/articles/consumer-privacy/new-california-law-to-require-additional-web-privacy-policy-disclosures/.

[10] *See generally* Susanna Kim Ripken, *The Dangers and Drawbacks of the Disclosure Antidote: Toward a More Substantive Approach to Securities Regulation*, 58 BAYLOR L. REV. 139, 147(2006) (calling for regulators to "lay aside the gospel of disclosure in favor of more substantive laws that regulate conduct directly").

III. *What's the Default Rule? Defaults rule, so policy decisions about choice defaults need to take into account whether an activity should be encouraged or deterred and the effects on the broader ecosystem if a certain used is restricted.*

Regardless of fine-tuning, the notice and choice mechanism presented to users is neither "value neutral" nor balanced. The discussion among policymakers has been captured by debate of exactly how notice should be offered and choice be made. Privacy discussions about whether consent should be solicited or opt-out choice provided focus solely on procedural mechanics, such as opt-in and opt-out, whether a box is pre-checked or not, central opt-outs and where they are located – on a web page, in a browser, in a browser's advanced settings, etc. The underlying premise is that "if users only knew – they would choose right."[11]

But users do not always "choose right." Collective action problems threaten to generate suboptimal outcomes where individuals fail to opt into societally beneficial data uses in the hope of free-riding on others' good will. Consider, for example, Internet browser crash reports, which very few users opt into;but when they do decline, they are often motivated less by real privacy concerns than by the belief that others will do the job for them. Additionally, consent-based default rules can be regressive because individual expectations fall back on existing experiences, not innovative potential. For example, if Facebook had not proactively launched its News Feed feature in 2006 and had instead waited for users to opt in, Facebook might never have grown as it has today. It is only when data started being distributed in a new way that users became accustomed to the change.

It is not the case that individuals should never be asked for express consent, rather the merits of a given data use need to be discussed as a broader societal issue. Consumers can certainly decide whether they want to get an email from a company or whether they want to share data publically. But asking consumers to express opinions on the use of web site analytics or uses that may be important to the function of a service is unlikely to be productive.

IV. Notice and The Challenge of Big Data. Notices shouldn't limit uses of data that can add great value while avoiding new risks.

The uses of Big Data can be transformative and may be difficult to anticipate at the time when data is initially collected.[12] These extraordinary benefits — including breakthroughs in medicine, data security, and energy use — can not be anticipated in a notice written long before a new concept is developed from analysis of data. Our concept of notice needs to anticipate that scientific analysis of data collected will depend on new types of analysis or use that haven't been clearly specified.

V. Notice and the Internet of Things: Sensors and tiny screens call for flexible models of notice.

Given the multiple inputs from sensors, geolocation technologies, collections of personal information and historical data, the unique aspects of the Internet of Things make simple application of the FIPPs a challenge. Data collection may occur without a screen to provide notice, may happen automatically and

[11] Omer Tene & Jules Polonetsky, *To Track or 'Do Not Track': Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 MINN. J.L. SCI. & TECH. 282 (2012).
[12] Jules Polonetsky & Omer Tene, Privacy and Big Data 66 STAN. L. REV. ONLINE 25

may collect data for a range of purposes. FPF provided input into the California Public Utilities Commission rulemaking for smart grid privacy and provides a smart grid privacy seal that helps implement these technologies in a way that integrate privacy and security into the world of connected devices.[13] FPF also recently published a White Paper in connection with the FTC workshop on the Internet of Things.[14]

One of the key lessons FPF learned during our work on the smart grid was that there is great need for flexibility in determining how notice and consent mechanisms should be presented to consumers activating smart grid devices. These devices could be operated by mobile apps or come in the form of a smart thermostat or a transistor on the side of a hot water tank. Some state utility commissions thought that notice of data practices should be provided by requiring that consumers provide formal consent, sometimes even in notarized form, before enabling a device to access smart meter data held by the utilities. This consent mechanism would have proven burdensome for consumers who wanted to purchase and easily activate their equipment.

The Internet of Things presents challenges. Meeting these challenges will require the establishment of standards and practices that are tailored to meet them without depriving the public of the considerable benefits of these technologies. Any "one-size-fits-all" approach would be inadvisable and likely counterproductive within the context of connected devices: "Any guideline or standard provided in this field should take . . . diversity into consideration and hence be context based and flexible."[15]

VI. Solutions can rely on transparency of algorithms, treating data use like a feature, advances in de-identification, serious self-regulation and effective privacy professionals.

There are many potential mechanisms companies can pursue to protect consumers and to offer them value for their data. Policymakers need to encourage creative approaches to addressing privacy challenges. FPF has proposed several ideas for places to start.

A. Transparency of the Algorithm

To minimize concerns of untoward data usage, organizations should disclose the logic underlying their decision-making processes to the extent possible without compromising their trade secrets or intellectual property rights. For example, individuals need to have some knowledge about the decisional criteria of organizations lest they face a Kafkaesque machinery that manipulates lives based on opaque justifications. While there remain practical difficulties of mandating disclosure without compromising a business' "secret sauce," a distinction can be drawn between proprietary algorithms, which would remain secret, and decisional criteria, which would be disclosed.

---

[13] *See Comments of the Future of Privacy Forum on the Proposed Decision Adopting Rules to Protect the Privacy and Security of the Electricity Usage Data of the Customers of Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company* (June 2, 2011), *available at* http://www.futureofprivacy.org/wp-content/uploads/2011/06/FPF_Cal_PUC_Smar_%20Grid_Comments.pdf;

[14] A New Privacy Paradign for the Internet of Things, Christopher Wolf & Jules Polonetsky, available at http://www.futureofprivacy.org/wp-content/uploads/Wolf-and-Polonetsky-An-Updated-Privacy-Paradigm-for-the-%E2%80%9CInternet-of-Things%E2%80%9D-11-19-2013.pdf

[15] REPORT ON THE PUBLIC CONSULTATION OF IOT GOVERNANCE, EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY 5-6 (2013).

B. Data Use "Featurization"

One promising path entails empowering individuals by granting them access to their personal data in intelligible, machine-readable form. Individuals would thus become active participants in the expanding data economy, analyzing their own information to improve their health, finances, career prospects, daily commutes and more. Mechanisms such as personal clouds or data stores will allow individuals to contract with third-parties who would get permission to selectively access certain categories of their data to provide further analysis or value-added services. We have called this the "featurization" of data, making data analysis a consumer-side application. Featurization will allow individuals to declare their own policies, preferences and terms of engagement, and do it in ways that can be automated both for them and for the companies they engage.[16]

C. Clarifying the Continuum between Personally Identifiable Information (PII) and Anonymity

Clarifying the scope of information subject to privacy law has become an increasingly important policy question. Personally identifiable information (PII) is one the central concepts in information privacy regulation, yet there is no uniform definition of PII.[17] Laws often turn on whether or not information is PII or not, and moreover, computer scientists have repeatedly shown that de-identified or anonymized data can be re-identified and linked to specific individuals. A bi-polar approach based on labeling information either "personally identifiable" or not has led to a constant arms race between de-identifiers and re-identifiers. PII should instead be defined based on a risk matrix taking into account the risk, intent, and potential consequences of re-identification, as opposed to a dichotomy between "identifiable" and "non-identifiable" data.

D. Self-Regulatory Efforts and Codes of Conduct

Self-regulatory codes of conduct may be an effective means for companies to honor consumer preferences in this rapidly evolving technology landscape. FPF has considerable experience working with companies to engage in meaningful self-regulation.

Recently, FPF identified location tracking in stores via mobile MAC addresses as an opportunity ripe for self-regulation. A MAC address is simply a 12-character string of letters and numbers; it doesn't contain personal information like your name, email address, or phone number. Nevertheless, because a MAC address is unique to each mobile device, analytics companies can use this information to generate reports about customer traffic in stores. For instance, retailers can learn how many unique customers walk into a store and the path shoppers take as they move throughout the store, and then use this information to improve the customer experience. While location analytics may provide any number of potential benefits to businesses and consumers, it is equally important that these practices are subject to privacy controls and are used responsibly.

Alongside seven leading location analytics providers and US Senator Charles Schumer, FPF announced an effort to establish guidelines and best practices to improve consumer privacy with location tracking

[16] *See* Doc Searls, *The Customer as a God*, WALL ST. J., July 20, 2012, *available at* http://online.wsj.com/article/SB10000872396390444873204577535352521092154.html.

[17] Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 NYU L. REV. 1814 (2011).

technologies.[18] Our proposal calls for the display of conspicuous signage by retailers and a central opt-out site for consumers. Our code of conduct requires companies to limit how the location information is used and shared and how long it may be retained. Data must be de-identified, and companies must explain in their privacy policy how they do so. Companies are required to get opt-in consent when personal information is collected, or when a consumer will be contacted, and the code calls for opt-out consent where the information collected is not personal. In addition, this data cannot be collected or used in an adverse manner for employment, health care or insurance purposes.[19] It is critical to give codes like this time to be implemented so their success can be assessed. Turning a code quickly into legislation will deter businesses that want to develop and promote best practices and would punish the companies who are ready to be progressive about setting new high standards.

E. Chief Privacy Officers and Privacy Review Boards

Having served as a Chief Privacy Officer for two leading internet companies and working today with more than 50 at FPF, I can tell you that privacy professionals are the front line in handling the nuanced and challenging issues that come up every day. Increasingly the issues faced aren't black and white legal disclosure issues, but rather nuanced issues of ethics, morality and judgement. Strengthening the role of these professionals, their training , seniority and capacity would be one of the most effective ways to deliver real privacy advances. One proposal that is getting attention is the implementation of institutional review boards (IRBs) that could help review and approve data projects that rely on consumer data.[20] In the context of Big Data, several scholars have proposed the use of "algorithmists" that could evaluate data sources, analytical tools, and any predictive results.[21] These roles could function like a board of directors or ombudsman in order to address problems and serve as a check on improper uses of data. While any analogy between traditional IRBs and a commercial review board has limits, industry increasingly faces ethical considerations over how to minimize data risks while maximizing benefits to all parties. Encouraging companies to create sophisticated structures and personnel to grapple with these issues would be invaluable. However, a legal requirement to have a particular form of internal corporate oversight is ill-advised, given the variation in size and purpose of various business organizations and data uses. The growth of the privacy profession is occurring organically, and government's role is to encourage rather than mandate that growth.

VII. Technology Solutions Are On the Way

In Sacramento, in Washington DC, and in Brussels policymakers frustrated with privacy challenges are seeking to advance "the right to be forgotten" or Eraser Buttons or other efforts to mandate rules for data. But companies in California are gaining traction with consumers by providing technologies that

---

[18] Press Release, Future of Privacy Forum, The Future of Privacy Forum and Sen. Schumer Announce Important Agreement to Ensure Consumers Have Opportunity to "Opt-Out" Before Stores Can Track Their Movement Via Their Mobile Devices (Oct. 22, 2013), http://www.futureofprivacy.org/2013/10/22/schumer-and-tech-companies-announce-important-agreement-to-ensure-consumers-have-opportunity-to-opt-out-before-stores-can-track-their-movement-via-their-cell-phones/.

[19] FUTURE OF PRIVACY FORUM, MOBILE LOCATION ANALYTICS CODE OF CONDUCT (Oct. 22, 2013), *available at* http://www.futureofprivacy.org/wp-content/uploads/10.22.13-FINAL-MLA-Code.pdf.

[20] VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK (2013).

[21] *See, e.g.*, Ryan Calo, *Consumer Subject Review Boards—A Thought Experiment*, 66 STAN. L. REV. Online 97 (2013); Robert Plant, *Ethical Data Collection: Please Have Your Boarding Card Ready*, BIG DATA REPUBLIC (Aug. 7, 2013), http://www.bigdatarepublic.com/author.asp?section_id=2635&doc_id=266293.

help ensure that data intended to be deleted doesn't stick around. SnapChat, once the favorite of teens now has a wide user base of millions who use it to send pictures that do not last. A popular new app called Frankly allows consumers to send texts that are ephemeral and automatically deleted in seconds. And while Do Not Track standards are debated, the recent iPhones and the newest Android phones already have an operation "Limit Ad Tracking" option that developers and ad networks are required to honor.

VIII. Conclusion

Louis Brandeis, who together with Samuel Warren "invented" the legal right to privacy in 1890, also wrote that "sunlight is said to be the best of disinfectants."[22] Privacy policies are one way to shine light on company data practices, but they need to be supported by new ways and new technologies to increase transparency and otherwise demystify what is happening to consumer's personal information. These new models need to be explored and tested over the upcoming years.

[22] Louis D. Brandeis, *Other People's Money and How the Bankers Use It* 92 (1914), *available at* http://www.law.louisville.edu/library/collections/brandeis/node/196.