COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

To

THE FEDERAL TRADE COMMISSION

Advertising and Privacy Disclosures in a Digital World

May 11, 2012

By notices published on February 29, 2012,[1] and May 2, 2012,[2] the Federal Trade Commission ("FTC") has requested original research or topics for discussion related to advertising disclosures in the online and mobile context to be examined at the workshop "Advertising and Privacy Disclosures in a Digital World" [hereinafter "Privacy Disclosure Workshop" or "FTC Workshop"]. The Privacy Disclosure Workshop is designed to update the "Dot Com Disclosure" guidelines that the Commission produced 12 years ago.[3] Pursuant to the Commission's notice, the Electronic Privacy Information Center ("EPIC") submits the following topics and questions to ensure that the workshop addresses the serious flaws that exist with a notice-centric approach to privacy protection.

EPIC is a public interest research center located in Washington, D.C. EPIC focuses on emerging privacy and civil liberties issues and is a leading consumer advocate before the FTC. EPIC has a particular interest in protecting consumer privacy and has played a leading role in developing the authority of the FTC to address emerging privacy issues and to safeguard the

[1] Press Release, Fed. Trade Comm'n, FTC Will Host Public Workshop to Explore Advertising Disclosures in Online and Mobile Media on May 30, 2012 (Feb. 29, 2012), http://www.ftc.gov/opa/2012/02/dotcom.shtm.
[2] Press Release, Fed. Trade Comm'n, FTC Announces Preliminary Agenda for Workshop about Advertising Disclosures in Online and Mobile Media (May 2, 2012), http://www.ftc.gov/opa/2012/05/dotcom_ma.shtm.
[3] *See* Fed. Trade Comm'n, Dot Com Disclosures: Information About Online Advertising (2000), *available at* http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus41.pdf.

privacy rights of consumers.[4] EPIC's 2010 complaint concerning Google Buzz provided the basis for the Commission's investigation and subsequent settlement concerning the social networking service.[5] In that case, the Commission found that Google "used deceptive tactics and violated its own privacy promises to consumers when it launched [Buzz]."[6] The Commission's recent settlement with Facebook was based on complaints filed by EPIC and other privacy and civil liberties organizations.[7] The Commission found that Facebook had "deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public."[8] EPIC also has an interest in alerting the Commission to the problems of "notice and choice," a policy approach that clearly favors the interests of businesses over consumers. In previous comments to the Commission, EPIC explained that notice and choice was a "failed model," as it was ineffective and failed to establish meaningful privacy safeguards.[9]

EPIC maintains that emphasizing notice or disclosure is an ineffective means of protecting the privacy rights of consumers. Privacy experts and social scientists have identified

---

[4] *See, e.g.*, Letter from EPIC Executive Director Marc Rotenberg to FTC Commissioner Christine Varney, EPIC (Dec. 14, 1995) (urging the FTC to investigate the misuse of personal information by the direct marketing industry), http://epic.org/privacy/internet/ftc/ftc_letter.html; DoubleClick, Inc., FTC File No. 071-0170 (2000) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf; Microsoft Corporation, FTC File No. 012 3240 (2002) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/consumer/MS_complaint.pdf; Choicepoint, Inc., FTC File No. 052-3069 (2004) (Request for Investigation and for Other Relief), http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.

[5] Press Release, Fed. Trade Comm'n, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network (Mar. 30, 2011), http://ftc.gov/opa/2011/03/google.shtm ("Google's data practices in connection with its launch of Google Buzz were the subject of a complaint filed with the FTC by the Electronic Privacy Information Center shortly after the service was launched.").

[6] *Id.*

[7] Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises (Nov. 29, 2011), http://ftc.gov/opa/2011/11/privacysettlement.shtm ("Facebook's privacy practices were the subject of complaints filed with the FTC by the Electronic Privacy Information Center and a coalition of consumer groups.").

[8] *Id.*

[9] EPIC, Comments to the FTC on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (2011), *available at* https://epic.org/privacy/ftc/EPIC_Comments_FTC_Internet_Privacy_Report.pdf.

several important flaws with a notice-centric approach to protecting privacy. Privacy notices must confront what Professor Helen Nissenbaum termed the "transparency paradox," where the clarity of a notice is in tension with its comprehensiveness. Privacy notices also do not address the "take it or leave it" basis on which most companies continue to offer privacy to consumers. Additionally, a host of cognitive and behavioral hurdles limit the effectiveness of even ideal notices. Further, companies routinely change privacy policies, making even the best efforts of consumers to operate within a notice and choice framework a waste of time. Finally, notices and disclosures do not provide any substantive protections for the privacy of consumers. As a result of these flaws, it is hardly surprising that consumers simply do not read privacy notices, privacy policies, or terms of service. Consumers are rational actors and understand that it is nonsensical to click through 100 privacy settings or read policy statements longer than the US Constitution when there is no practical benefit to them. Similarities between mobile advertising and traditional digital contexts suggest that an approach that emphasizes notice for mobile advertisements will suffer from the same flaws. Indeed, to the extent that the mobile context is unique, its unique features only heighten the flaws that privacy disclosures must confront.

On the other hand, the President has recently set our a comprehensive framework for privacy protection – the Consumer Privacy Bill of Rights – that avoids many of the shortcomings of the "notice and choice" approach.[10] Under the Consumer Privacy Bill of Rights, companies that collect and use personal data on consumers would necessarily take on privacy responsibilities and consumers who provide personal data to companies would gain new rights. This approach is also technology-neutral and forward-looking: it applies as directly to mobile apps as it does to web-based services.

[10] White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy, 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf [hereinafter White House, CPBR].

In order to ensure that the Commission develop meaningful safeguards for users of new mobile-based services, EPIC recommends that the FTC revise the schedule of the workshop to set aside time to address the central question of how best to establish the Consumer Privacy Bill of Rights for mobile services. EPIC believes that a very good panel discussion on this topic, incorporating a wide range of views, could help the Commission move forward in one of the key areas for online privacy,

To the extent that the FTC is still interested in pursuing the notice-based model, which EPIC believes is a mistake, we recommend:

- The workshop should address the "transparency paradox";
- The workshop should consider the effectiveness of layered notices similar to that recommended by the Article 29 Working Party;
- The workshop should address the effectiveness of "visceral," or nonverbal, approaches to notice;
- The workshop should address the ways in which transparency might reduce the adhesive nature of privacy notices through, for example, access and correction rights;
- The workshop should address the behavioral and cognitive limitations facing consumers;
- The workshop should address whether interface design can alleviate these behavioral and cognitive limitations;
- The workshop should address the connection between disclosure and a broader regime of privacy protection.

A careful examination of these two approaches – a "Bill of Right" versus "Notice and Choice" – is likely to reveal that the rights-based approach is consistent with other efforts to proect privacy and will be far more effective.[11]

[11] *See generally*, Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2011 STAN. TECH. L. REV. 1 (2001).

I. The Workshop Should Address the "Transparency Paradox," as well as Efforts to Alleviate it Through Layered or Visceral Notice

Attempts to notify or disclose privacy practices must contend with what Professor Helen Nissenbaum has called the "transparency paradox":

> Achieving transparency means conveying information-handling practices in ways that are relevant and meaningful to the choices individuals must make. If notice (in the form of a privacy policy) finely details every flow, condition, qualification, and exception, we know that it is unlikely to be understood, let alone read. But summarizing practices in the style of, say, nutrition labels is no more helpful because it drains away important details, ones that are likely to make a difference: who are the business associates and what information is being shared with them; what are their commitments; what steps are taken to anonymize information; how will that information be processed and used. An abbreviated, plain-language policy would be quick and easy to read, but it is the hidden details that carry the significance.[12]

Currently, there is abundant evidence to indicate that efforts to notify consumers fail to achieve either clarity or comprehensiveness, the two goals that Professor Nissenbaum placed in tension above. Privacy notices are long and frequently incomprehensible. It would take consumers 76 working days to read the privacy policies they encounter in one year.[13] If consumers were to actually read every privacy policy, the opportunity cost to the national economy would be $781 billion.[14] And should consumers wish to attempt to read the privacy notices they encounter, many would be unable to understand them. In 2004, researchers analyzed the content of the privacy policies of 64 popular websites and found that

> Of the 64 policies examined, only four (6%) were accessible to the 28.3% of the Internet population with less than or equal to a high school education. Thirty-five

[12] Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140(4) DAEDALUS 32, 36 (2011) *available at* http://www.amacad.org/publications/daedalus/11_fall_nissenbaum.pdf. Stanford's Ryan Calo explained the paradox in similar terms: "Notice is, in this sense, hydraulic: it is very difficult to convey complex content in a clear and concise format." Ryan Calo, *Against Notice Skepticism in Privacy (And Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1056 (2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1790144&download=yes.

[13] *See* Alexis Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC (Mar. 1, 2012), http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/; *see also* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S J. L. & POL'Y FOR INFO. SOC'Y 543, 544, 564 (2008).

[14] Madrigal, *supra* note 13.

> policies (54%) were beyond the grasp of 56.6% of the Internet population, requiring the equivalent of more than fourteen years of education. Eight policies (13%) were beyond the grasp of 85.4% of the Internet population, requiring the equivalent of a postgraduate education.[15]

Companies that have attempted to make their privacy practices clear and understandable have often failed to provide the level of detail necessary for a complete understanding of their practices. Most notably, On January 24, 2012, Google announced that, effective March 1, the company will change its terms of service, and use the personal information obtained from user in ways inconsistent with the original collection.[16] The media praised Google's new policy for being written in "plain English."[17] However, Google's simplified terms of service omitted important information. A complaint by EPIC argued that "Google's privacy policy also fails to adequately explain the way in which users' consolidated data will be used for targeted advertising" and that it "fail[s] to disclose that users can limit the aggregation of their personal information."[18] Similarly, the Center for Digital Democracy stated that "Google fails to tell users in its principal privacy change communications how such data collection, profiling, and targeting practices impact — and potentially harm — their privacy."[19] And the French Data Protection Authority CNIL echoed these observations, informing Google that

> The new privacy policy provides only general information about all the services and types of personal data Google processes. As a consequence, it is impossible

[15] Carlos Jensen and Colin Potts, Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '04). ACM, New York, NY, USA, 471-478 (2004), *available at* http://lib.zstu.edu.cn/res_base/lib_com_www/upload/article/file/2010_3/7_12/f4ywgbiwtpjn.pdf.

[16] Alma Whitten, *Updating our privacy policies and terms of service*, THE GOOGLE BLOG (Jan. 24, 2012), http://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html.

[17] *See, e.g.*, Jessica Guynn, *Google plans to merge more user data across its products*, L.A. TIMES (Jan. 24, 2012), http://latimesblogs.latimes.com/technology/2012/01/google-plans-to-merge-more-user-data-across-its-products.html.

[18] *See Elec. Privacy Info. Ctr. v. F.T.C.*, No. 12-0206 ABJ, 2012 WL 593063 (D.D.C. Feb. 24, 2012) aff'd, 12-5054, 2012 WL 1155661 (D.C. Cir. Mar. 5, 2012) (Mtn. for Temp. Restraining Order and Prelim. Inj.) *available at* https://epic.org/privacy/ftc/google/TRO-Motion-final.pdf.

[19] Ctr. for Digital Democracy, Google, Inc., Request for Investigation and Imposition of Fines and Other Remedies for Violation of "Google Buzz" Consent Decree (2012), *available at* http://www.centerfordigitaldemocracy.org/sites/default/files/CDDGoogleComplaint022212.pdf.

> for average users who read the new policy to distinguish which purposes, collected data, recipients or access rights are currently relevant to their use of a particular Google service.[20]

CNIL suggested that Google adopt a form of layered notice similar to that suggested by the Article 29 Working Party in Opinion 10/2004,[21] where "basic information may be delivered in a short notice (layer 1) but more detailed information is provided in the condensed and full notices (layer 2 and 3)."[22]

Several characteristics of the mobile context heighten the transparency paradox. First, modern smartphones are equipped with far more sensors than traditional computers, and thus are able to collect additional types of information. Most significantly, smartphones enable comprehensive location tracking that can reveal sensitive information about a person's social, professional, and personal identity.[23] Many smartphones also contain other sensors, such as barometers, accelerometers, and altimeters.[24] These additional categories of data would presumably have to be disclosed somehow in order to achieve comprehensibility. Doing so, however, would add to the length and complexity of the notice.

Second, smartphones are limited by the physical size of the screen. Although screen sizes are increasing, nearly all smartphones have screens smaller than 5 inches.[25] This places obvious limitations on the amount of information that can be conveyed on a single screen. More

[20] Letter from Isabelle Falque-Pierrotin to Larry Page regarding Google's new privacy policy, Feb. 27, 2012, *available at* https://epic.org/privacy/ftc/google/Courrier-Google-CE121115-27-02-2012.pdf.
[21] Article 29 Data Protection Working Party, Opinion 10/2004 on More Harmonised Information Provisions (2004),http://www.cnpd.public.lu/en/publications/groupe-art29/wp100_en.pdf.
[22] Letter from Isabella Falque-Pierrotin, *supra* note 20. Ryan Calo has offered support for a similarly layered approach that incorporates his concept of visceral notice, where visceral notice would be given to ordinary consumers, and detailed technical notice would be available to regulators, journalists, and privacy professionals. *See* Calo, *supra* note 12, at 1062.
[23] *See* Amicus Curiae Brief of Electronic Privacy Information Center (EPIC), *In re: Application of the United States of America for Historic Cell Site Data*, No. 20884 (5th Cir. Mar. 16, 2012), *available at* https://epic.org/amicus/location/cell-phone-tracking/EPIC-5th-Cir-Amicus.pdf.
[24] *See, e.g.*, Dan Nosowitz, *So, Um, Why Does the New Google Phone Have a Barometer in It?*, POPSCI (Oct. 19, 2011), http://www.popsci.com/gadgets/article/2011-10/so-um-why-does-new-google-phone-have-barometer-it.
[25] Matt Hamblen, *Smartphone Screens are Getting Bigger*, COMPUTERWORLD (May 3, 2012), https://www.computerworld.com/s/article/9226796/Smartphone_screens_are_getting_bigger_.

information can be presented on multiple screens, but a multi-screen approach reduces the clarity and simplicity of the notice.

Additionally, privacy on a mobile device involves a broad range of actors. Privacy on a typical smartphone implicates the business practices of a hardware manufacturer, a carrier, a platform developer, an application developer, and a 3rd-party advertising or analytics network, each of whom might have advertising practices that require disclosure.[26] Owning a smartphone could require its owner to simultaneously monitor the privacy practices of Samsung, Sprint, Google, Zynga, and Admob (Google). The information flows between these actors creates further problems for simple, clear disclosures.

Some scholars have tried to rehabilitate notice and solve the transparency paradox by relying on nonverbal, or "visceral" notice. Ryan Calo, Director of Privacy and Robotics at Stanford's Center for Internet and Society, describes visceral notice as "leverage[ing] a consumer's very experience of a product or service to warn or inform" rather than "describing practices in language or symbols."[27] Calo offers three categories of visceral notice: (1) "familiarity with one technology or context to warn or inform about another"; (2) "using certain common psychological reactions to design to change a consumer's mental model of a product or service"; and (3) "demonstrating the result of company practices for the specific consumer, rather than describing the practices themselves."[28] For example, the shutter sound produced by cameras on mobile phones is an example of the first kind of visceral notice. Unlike analog cameras, digital cameras need not produce an audible sound when a picture is taken. However, "[b]y hearing the clicking sound issuing from the camera, the subject instantaneously realizes

[26] *See* Ashkan Soltani, Everything I Know About Mobile Privacy in 30min or Less (Apr. 13, 2012), http://www.law.nyu.edu/ecm_dlv4/groups/public/@nyu_law_website__centers__information_law_institute/documents/documents/ecm_pro_072600.pdf.
[27] Calo, *supra* note 12, at 1033.
[28] *Id.* at 1033-34. For an example of design changes, the second kind of visceral notice, see *infra* Part III.

that she is in the presence of a recording technology."[29] Calo considers the Dashboard and Ads Preferences manager offered by Google, as well Yahoo's Ad Interest Manager, to be examples of the third kind of visceral notice: "[t]hese tools, while imperfect, show users how their information is actually used, as opposed to merely telling them how it might be used."[30] It is unclear, however, whether a form of visceral notice exists that could make consumers aware of the complex flow of information involved in mobile or online advertising.

Accordingly, EPIC recommends that the workshop address the transparency paradox. The workshop should also consider the effectiveness of layered notices similar to that recommended by the Article 29 Working Party, and the effectiveness of visceral approaches to notice similar to those described above.

II. The Workshop Should Address the Ways in Which Transparency Might Reduce the Adhesive Nature of Privacy Notices

Another flaw of a notice-centric approach to privacy is that operates as part of an adhesive, "take it or leave it" regime. Once a company's privacy practices are disclosed, the consumer's choice is either to accept them entirely or not at all. The Commission has criticized the adhesiveness involved in privacy notices in its most recent report, writing that "a 'take it or leave it' approach is problematic from a privacy perspective, in markets for important services where consumers have few options."[31]

Although disclosure is no substitute for actual, substantive privacy protections such as those outlined below, many privacy regimes have incorporated a principle of transparency that gives consumers greater participation in the storage and use of their personal information. The Fair Credit Report Act gives consumers the right to access information about them that is held by

[29] *Id.* at 1037
[30] *Id.* at 1043-44
[31] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

credit reporting agencies as well as the right to have errors or discrepancies investigated and corrected by the credit reporting agencies.[32] The White House's Consumer Privacy Bill of Rights contains an "Access and Accuracy" principle that provides "a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate."[33] The Council of Europe Convention 108 gives individuals the right to "rectification or erasure of such data if these have been processed contrary to the provisions of domestic law" and the right to a remedy if a request for confirmation or communication is denied. [34] Indeed, the European Union's Proposed Data Protection Regulation even includes the right to demand erasure of personal data.[35] By extending disclosure beyond the initial point of purchase, these regimes provide a greater role for consumers in the management of their personal information.

Accordingly, the workshop should discuss how transparency or disclosure can be implemented to help offset the adhesive nature of privacy agreements, such as through the creation of a right to access and correct personal data.

III. The Workshop Should Examine Whether Notice Can Be Given in a Manner That Lessens the Impact of Consumers' Behavioral and Cognitive Biases

Behavioral and cognitive science studies suggest that even when confronted by ideal notices, consumers suffer from several limitations that impede their ability to act optimally with regard to privacy. Alessandro Acquisti, associate professor at the Heinz College, Carnegie Mellon University, has conducted behavioral decision research that identifies and illuminates the

[32] *See* 15 U.S.C. § 1681g.
[33] White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy, Feb. 23, 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf
[34] Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data CETS No.: 108, *available at* http://conventions.coe.int/treaty/en/treaties/html/108.htm.
[35] *Commission Proposal for a Regulation of the European Parliament and of the Council*, art. 4(2), COM (2012) 11 final (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

hurdles consumers face when evaluating privacy trade-offs.[36] Professor Acquisti explained that consumer decision-making is affected by asymmetric information, bounded rationality, and cognitive and behavioral biases.[37]

Asymmetric information describes the fact that consumers are often poorly-informed about the collection and usage of their personal information relative to the companies that collect and use that information.[38] Bounded rationality refers to limitations in the ability of consumers to process information and formulate rational plans for solving complex problems.[39] The limits of rationality are exacerbated by technological developments that pose privacy risks that were not foreseen at the time of data collection, thus making them practically impossible to account for when deciding whether to consent to the privacy practices of a particular business.[40] Finally, several well-known cognitive and behavioral biases include: (1) the instant gratification bias that results from the tendency of human beings to value the present more than the future, thus leading consumers to disclose information in the present that might subject them to future privacy risks; (2) the paradox of control in privacy decision making that results when increased feelings of control over the release of personal information elicit greater disclosure of sensitive information and more elevated privacy risks; and (3) interface alterations that can induce consumers to disclose more information, such as "showing that other individuals have made sensitive

[36] *See Understanding Consumer Attitudes About Privacy: Hearing Before the Subcomm. on Commerce, Manufacturing, and Trade of the House Comm. on Energy and Commerce* (Oct. 13, 2011) (testimony of Prof. Alessandro Acquisti) http://republicans.energycommerce.house.gov/Media/file/Hearings/CMT/101311/Acquisti.pdf.
[37] *Id.* at 2
[38] *Id.* at 4.
[39] *Id.* at 5
[40] *Id.* To illustrate this point, Professor Acquisti described research conducted at Carnegie Mellon University that allowed him to predict individuals' Social Security Numbers using simple demographic data made available by the individuals themselves through their social media profiles. He also discussed a study in which individuals were identified in public using face recognition technologies and photos made publicly available by the targets on social networking sites. Data aggregation also creates unforeseeable privacy risks. Target, for example, was able to accurately infer the pregnancy status and due date of consumers using relatively nonsensitive purchase information of about 25 products. *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all.

disclosures," "asking questions covertly so that the act of disclosing is not salient," or "altering the order in which questions of varying sensitivity are asked."[41]

Even assuming that perfect notice is able to cure information asymmetries and ease the demands of information processing and planning, the other cognitive and behavioral biases remain. Experts have identified other cognitive and behavioral limitations. Consumers are biased in favor of limiting the cognitive effort involved in decision-making.[42] Thus, greater disclosure is unlikely to lead to more accurate decision-making because "[e]xcept for the most obviously sensitive information, people are not likely to expend the cognitive effort necessary to weigh the pros and cons."[43] Decisions made under time constraints are also problematic. Consumers faced with a time-sensitive decision, or the appearance of one, employ simpler decision-making strategies.[44] Most decisions made on the Internet occur under perceived time constraints, as users are asked to consent to business practices knowing that they often cannot enjoy the benefits of a product or service until they do so. As Ed Felten, the Commission's Chief Technologist, stated "[g]iven the choice between dancing pigs and security, users will choose dancing pigs every time."[45]

Finally, consumers reach better decisions when their decisions produce concrete and immediate feedback.[46] The consequences of privacy-related decisions, however, are often distant. Feedback may come years later in the form of identity theft or a lower credit rating, if it comes at all. "Only rarely will someone be able to trace the spam, identity theft, profiling, pop up

[41] Acquisti, *supra* note 36, at 6.
[42] James P. Nehf, *The FTC's Proposed Framework for Privacy Protection Online: A Move Toward Substantive Controls or Just More Notice and Choice?*, 31 WILLIAM MITCHELL L. REV. 1727 (2011).
[43] *Id.*
[44] *Id.*
[45] Mozilla Security Review and Best Practices Guide, http://www.mozilla.org/projects/security/components/reviewguide.html.
[46] Nehf, *supra* note 42.

advertisement, junk mail, or other effects of information sharing to a particular data collector's privacy practices."[47] When the consequences of a decision are difficult to determine, consumers are unlikely to invest in accurate decision-making strategies.

Interface design could induce consumers to give greater consideration to privacy issues. For example, Ryan Calo's second category of visceral notice involves changing the design of a product or service to achieve specific policy goals.[48] Anthropomorphic qualities such as faces or eyes could be introduced to increase consumer awareness of tracking or surveillance.[49] Specifically, Calo imagines a situation where "each advertising network on the Internet had an avatar that ran onto the bottom of the screen to denote the fact that the network was following the user. Users could click on the Avatar to opt out of tracking (or to hide the avatar if they find it annoying)."[50] Studies have also shown that interface formality affects the willingness of consumers to divulge information, with consumers disclosing more information on casual websites than formal ones.[51] A formal, as opposed to a casual, design could help "place the consumer on their guard" as to data collection and sharing practices.[52]

Accordingly, the workshop should address the behavioral and cognitive limitations facing consumers. The workshop should also address whether interface design can alleviate these behavioral and cognitive limitations.

IV. The Workshop Should Address the Connection Between Disclosure and a Broader Regime of Privacy Protection

Finally, the fundamental flaw with a notice-centric approach to protecting privacy is that notice is not a substantive form of protection but a procedural one. Notice, by itself, does not

[47] *Id.* at 17.
[48] Calo, *supra* note 12.
[49] *Id.* at 1039
[50] *Id.* at 1040.
[51] *Id.* at 1046.
[52] *Id.* 1040.

dictate any limitations on the collection, storage, manipulation, or dissemination of information. For example, Facebook recently revised its Statement of Rights and Responsibilities to clarify that "[w]hen you or others who can see your content and information use an application, your content and information is shared with the application."[53] Assuming that placing a provision in the Statement of Rights and Responsibilities constitutes adequate notice or disclosure, Facebook's statement did not address the underlying practice. The objection that many users had was not to the fact that Facebook's previous disclosure had been inadequate, but to the substance of the data-disclosure practice itself. This is evident in the comments of users like Abine's Sarah Downey: "If I do not explicitly give an app permission to access my information, it should not have access to my information."[54]

Because even the best notice cannot provide substantive privacy protections for consumers, most privacy regimes treat notice as only one aspect of a more comprehensive set of protections. The Privacy Act, for example, sets forth the following requirements:

> (1) Permit an individual to determine what records pertaining to him are collected, maintained used or disseminated by such agencies;
> (2) Permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;
> (3) Permit an individual to gain access to information pertaining to him in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records;
> (4) Collect, maintain, use or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;
> (5) Permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and

[53] Facebook, Statement of Rights and Responsibilities Update, https://www.facebook.com/note.php?note_id=10151420037600301.
[54] *Id.* (comments of Abine, Inc.).

> (6) Be subject to civil suit for any damages which occur as a result of willful or intentional action which violates any individual's rights under this Act.[55]

Similarly, the Organization for Economic Cooperation and Development (OECD) Privacy Guidelines include: data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.[56] The Council of Europe Convention 108 contains principles regarding data quality, sensitive data categories, data security, and transborder data flows.[57] The White House's recent Consumer Privacy Bill of Rights enumerates seven principles: Individual Control, Transparency, Respect for Context, Security, Access and Accuracy, Focused Collection, Accountability.[58] Even the Commission's framework, which relies more heavily upon notice and disclosure, still includes the principles of privacy by design and choice.[59]

Although procedural protections like notice and transparency are conceptually distinct from the substantive protections outlined above, the two types of protections are nevertheless mutually supportive and interrelated. Responding to claims that notice-centric regimes have been successful in the health care context, Professor Helen Nissenbaum explains that

> In my view, these protocols work not because they have found the right formulation of notice and the authentic mechanism for consent but because they exist within a framework of supporting assurances. . . . We trust the long years of study and apprenticeship that physicians undergo, the state and board certifications, peer oversight, professional codes, and above all, the system's interest (whatever the source) in our well-being. We believe in the benevolence of institutions of higher learning and, in large part, their mission to promote human welfare. Far from perfect, and subject to high-visibility breaches, the systems that constitute these safety nets have evolved over centuries; they undergird and

[55] Privacy Act of 1974, 5 USC § 552a.
[56] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, *available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.
[57] Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data CETS No.: 108, *available at* http://conventions.coe.int/treaty/en/treaties/html/108.htm
[58] White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy, Feb. 23, 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf
[59] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

> warrant the consent agreements that patients and subjects confront every day. In the online environment, by contrast, individual consent agreements must carry the entire weight of expectation.[60]

In other words, a look behind the success stories reveals that notice works to the extent that it is supported by substantive protections.

Accordingly, the workshop should address the connection between disclosure and a broader regime of privacy protection. Specifically, the workshop should consider how best to establish the Consumer Privacy Bill of Rights for advertising on mobile services.

VI. Conclusion

As a means of safeguarding privacy, notice presents a host of difficult problems. Thus, the Commission should ensure that the above issues are raised and adequately addressed at the workshop. A better approach, though, is to focus on the implementation of the Consumer Privacy Bill of Rights, recently set out by the White House.

Respectfully Submitted,

Marc Rotenberg
EPIC Executive Director

David Jacobs
EPIC Consumer Protection Fellow
Electronic Privacy Information Center
1718 Connecticut Ave. NW Suite 200
Washington, DC 20009
202-483-1140 (tel)
202-483-1248 (fax)

[60] Nissenbaum, *supra* note 12, at 36.