COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

To

THE FEDERAL TRADE COMMISSION

In Short: Advertising and Privacy Disclosures in a Digital World

FTC Project No P114506

July 11, 2012

The Federal Trade Commission ("FTC") has requested public comments on the issues raised at the workshop "In Short: Advertising and Privacy Disclosures in a Digital World," [hereinafter "In Short Workshop" or "FTC Workshop"]. Pursuant to this request, the Electronic Privacy Information Center ("EPIC") submits these comments and recommendations to ensure that the Commission's approach to disclosure addresses the 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 privacy rights of consumers.[1] EPIC's 2010 complaint concerning Google Buzz provided the basis for the Commission's investigation and subsequent settlement concerning the social

[1] *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.

networking service.[2] In that case, the Commission found that Google "used deceptive tactics and violated its own privacy promises to consumers when it launched [Buzz]."[3] The Commission's recent settlement with Facebook was based on complaints filed by EPIC and other privacy and civil liberties organizations.[4] 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."[5] 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 did not establish meaningful privacy safeguards for consumers.[6]

EPIC submitted comments to the Commission before the In Short Workshop.[7] EPIC first urged the Commission to discuss the connection between notice and a substantive regime of privacy protection such as that found in the Consumer Privacy Bill of Rights.[8] EPIC also suggested that the workshop address the well-known flaws with notice—such as Helen Nissenbaum's "transparency paradox"—and discuss "visceral" or nonverbal approaches to

[2] 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.").
[3] *Id.*
[4] 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.").
[5] *Id.*
[6] 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.
[7] EPIC, Comments to the FTC on In Short: Advertising and Privacy Disclosures in a Digital World (2012), *available at* https://epic.org/privacy/ftc/EPIC-FTC-Ad-Disclosures-FINAL.pdf.
[8] *Id.* at 13-16.

notice.[9] The In Short Workshop did not address substantive privacy protections, and addressed visceral notice only briefly. Much of the workshop's privacy notice section was devoted to the presentation of new privacy icons or labels.[10] Because privacy icons are subject to many of the same flaws as traditional privacy notices, these comments review the objections to notice-centric privacy frameworks that were discussed in greater detail in EPIC's previous comments on this workshop. Furthermore, because the workshop did not discuss substantive privacy protections, EPIC renews its request that the Commission consider substantive privacy protections in addition to procedural guidelines such as notice policies. To the extent the Commission is focused on disclosure, EPIC recommends broadening its conception of disclosure to include principles of meaningful transparency and access that would allow consumers to determine the actual personal information about them that is collected by advertisers.

I. A Notice-Based Privacy Regime Provides Inadequate Protection For Consumers

A notice-based privacy regime shifts the burden of protecting privacy to the consumer, but the practical obstacles of restricting the use of one's data are excessively burdensome. Significantly, privacy policies often do not reach the intended audience. Most consumers, even those that care about privacy, choose not to read privacy policies.[11] Consumers do not have the time to read all of the privacy notices they encounter.[12] Moreover, consumers may be unaware of the complex flow of information implicated in the use of a smartphone: To ensure the privacy of her consumer data, the typical smartphone consumer would need to read, understand, and act

[9] *Id.* at 5-9.
[10] *See* FED'L TRADE COMM'N WORKSHOP TRANSCRIPT: ADVERTISING AND PRIVACY DISCLOSURES IN A DIGITAL WORLD: MOBILE PRIVACY DISCLOSURES (May 30, 2012), *available at* http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/053012_FTC_sess4.pdf.
[11] M. Ryan Calo, *Against Notice Skepticism in Privacy (And Elsewhere)*, 87 NOTRE. DAME. L. REV. 1027, 1033 (2012).
[12] *See* 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/; Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S J. L. & POL. FOR INFO. SOC'Y 543, 544, 564 (2008).

upon the privacy policies of different actors, including but not limited to the hardware manufacturer, the carrier, the platform developer, app developers, and third party advertising or analytics networks.[13] Additionally, as Kevin Trilli observed during Session 4 of the FTC Workshop, if consumers encounter too many privacy policies with too much information, they will become frustrated and fatigued, causing them "tune out even further."[14]

Those consumers that do read privacy notices often find them unclear or excessively long. As Professors Aleecia McDonald and Lorrie Faith Cranor have pointed out, privacy policies frequently take more ten minutes to read.[15] Although the average American reads at an eighth- or ninth-grade reading level, privacy notices are often written at a college reading level or, worse, in "legalese."[16] Therefore, consumers who read privacy policies may, on a practical level, be unable to protect the flow of their consumer information.

A notice-based privacy regime fatally relies upon a false model of human capacity.[17] Notice-based privacy works under the assumption that consumers are perfectly rational actors with limitless attention.[18] However, cognitive biases impede consumer comprehension of privacy policies.[19] For example, consumers' ability to process information in a privacy policy is affected by information overload: faced with too much data, consumers tend to make inferior decisions because they become distracted by less relevant information at the expense of

[13] *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.
[14] FED'L TRADE COMM'N WORKSHOP TRANSCRIPT: ADVERTISING AND PRIVACY DISCLOSURES IN A DIGITAL WORLD: MOBILE ADVERTISING DISCLOSURES 19 (May 30, 2012), *available at* http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/FTCindex.html#May30_(comments of Ilana Westerman, Principle, Create with Context).
[15] McDonald & Faith Cramer, *supra* note 12, at 544.
[16] Calo, *supra* note 11.
[17] *Id*. at 1053.
[18] *See id.*
[19] *See id.*

understanding highly relevant information.[20] In the sense of welfare maximizing, it may be rational for consumers to ignore privacy policies because "having to read a notice takes the consumer away from fun or function of a service. People are busy and face many competing demands on their time."[21] Additionally, companies may carefully write privacy policies to take advantage of other cognitive biases, such as anchoring and framing, to make their privacy policies seem more advantageous than they truly are.[22]

Finally, a notice-based privacy regime does not provide substantive requirements or guidelines necessary to protect consumer privacy. A privacy policy only protects consumer data to the extent that the company has elected to provide substantive protections. Because many companies believe it is not in their economic interest to do so, privacy policies often offer only illusory protects or, worse, are up front about their lack of protection. Often, consumers are presented with a "take-it-or-leave-it" option: They must consent to the collection, use, and dissemination of their data or forgo the service or product altogether.[23]

II. Privacy Labels or Icons Suffer From Many of the Same Flaws as Traditional Privacy Notices

The In Short Workshop's discussion of mobile privacy disclosures focused on several privacy icons or labels. The panel featured presentations about Create with Context, Inc.'s trust icon,[24] Association for Competitive Technology's privacy-disclosure icon,[25] and an icon created by PrivacyChoice's Policymaker.[26] As with traditional privacy notices, these icons suffer from several problems. First, as with privacy notices, consumers are unlikely to make use of them.

---

[20] *See id.*
[21] Calo, *supra* note 11, at 1052.
[22] *See id.*
[23] FED'L. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 50-51 (2012).
[24] *See* ADVERTISING AND PRIVACY DISCLOSURES IN A DIGITAL WORLD: MOBILE PRIVACY DISCLOSURES, *supra* note 10, at 7.
[25] *See id.* at 16.
[26] *See id.* at 19.

Most consumers, even those that care about privacy, choose not to read privacy policies.[27] Like traditional privacy policies, privacy icons are likely to be ignored. For example, the Digital Advertising Alliance's (DAA) ad-based icon is clicked on by only 0.0035 percent of users.[28] At the workshop, Lorrie Faith Cranor conducted research that "put ads before 1,500 people that had this [privacy] icon. And the vast majority of them didn't recognize having ever seen it before, although surely they had."[29]

More importantly, by sacrificing comprehensiveness for clarity, privacy icons fail to overcome Helen Nissenbaum's transparency paradox: "summarizing practices in the style of, say, nutrition labels is no more helpful [than an exhaustive privacy policy] because it drains away important details, ones that are likely to make a difference."[30] The lack of comprehensiveness is especially problematic because the use of smartphones involves a complex flow of information. A privacy icon has little hope of adequately explaining the privacy practices of the hardware manufacturer, the carrier, the platform developer, the app developers, the third-party advertising networks, much less the relationships between all of them. Ultimately, as Lorrie Faith Cranor pointed out, "privacy is not a concept that lends itself to little pictograms very well."[33]

---

[27] Calo, *supra* note 11, at 1033.
[28] *The Need for Privacy Protections: Is Self-Regulation Adequate?: Hearing Before the S. Comm. on Commerce, Science and Transportation*, 112th Cong. 4-5 (2012) statement of Alex Fowler, Chief Privacy Officer, Mozilla), *available at* http://defendourfreedoms.net/files/4/2/6/6/5/166425-156624/Fowler_Testimony.pdf.
[29] ADVERTISING AND PRIVACY DISCLOSURES IN A DIGITAL WORLD: MOBILE PRIVACY DISCLOSURES, *supra* note 10, at 14.
[30] 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.
[33] *See* ADVERTISING AND PRIVACY DISCLOSURES IN A DIGITAL WORLD: MOBILE PRIVACY DISCLOSURES, *supra* note 10, at 14. Although EPIC believes that privacy icons are not an adequate form of disclosure, this is not to say that the Commission should abandon all efforts at nonverbal notice. To the extent that the FTC is committed to pursuing a notice-based privacy regime, EPIC reiterates its suggestion that companies make disclosure more effective and mitigate the burden on consumers seeking to protect their data by implementing visceral notice. Although only briefly discussed at the workshop, visceral notice improves comprehension of data use. Visceral notice utilizes aural or visual signals to help the consumer understand intuitively when data is collected by "showing" consumers rather than "telling" them in text and using signals familiar to the consumer. *See* Calo, *supra* note 11, at 1033. For

Further, privacy safeguards are not easily reduced to metrics as are vitamins and calories on a nutritional label or miles per gallon on an auto sticker. Without the ability to quickly and easily translate the information contained in a privacy "short notice" or icon into meaningful and stable values, little meaningful information is actually conveyed to the consumer.[34] There is the additional problem that notices are always subject to change. Consumers who attempt to act on the information provided by a privacy notice or icon may subsequently find that their preferences are ignored as new business practices emerge.[35] As Professor Alessandro Acquisti has noted, consumers are less likely to take affirmative measures to protect their privacy when they expect that their privacy will not be protected.[36] This is an additional reason that substantive roles that regulate business practices are preferable to notice-based regimes.

III. The Commission's Conception of Disclosure Should Include Transparency in Addition to Notice

The In Short Workshop focused on *notice*, or mechanisms for transmitting information at or before the point of purchase. The Commission should ensure that its conception of disclosure also includes *transparency*, or mechanisms for transmitting information throughout the remainder of the consumer's interaction with a product or service. Meaningful transparency can facilitate greater user control over their personal information held by others in ways that are not possible (or are difficult) to accomplish using notice. For example, Mozilla's browser add-on,

---

example, companies can alert the consumer in real time to the flow of information about the consumer by using a red, flashing light in the corner of the webpage, much like a recording light on a video camera, to show the consumer when data is being collected. The FTC should devote attention to the advantages of visceral notice over traditional notice.

[34] EPIC, Comments to the FTC on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (2011), at 17-18, *available at* https://epic.org/privacy/ftc/EPIC_Comments_FTC_Internet_Privacy_Report.pdf.

[35] *See id.* at 9 (discussing changes to Facebook's privacy policy that breached the users' expectations of privacy).

[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.

Collusion, provides consumers with real-time information about third parties who are collecting their information online.[37] The resulting "spider-web of interaction between companies and other trackers" conveys real-time, visual information in a way that prior notice could not accomplish.

When transparency is combined with the right to ensure accuracy, the result is even more favorable to consumers. Many privacy regimes have incorporated a principle of transparency that gives consumers greater participation in the storage and use of their personal information. Although disclosure is no substitute for actual, substantive privacy protections such as those outlined below, it can still benefit consumers. For example, The Fair Credit Report Act gives consumers the right to access information about them that is held by credit reporting agencies as well as the right to have errors or discrepancies investigated and corrected by the credit reporting agencies.[38] 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."[39] 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.[40] Indeed, the European Union's Proposed Data Protection Regulation even includes the right to demand erasure of personal data.[41] By extending disclosure beyond the initial point of purchase, these regimes provide a greater role for

[37] *Introducing Collusion*, https://www.mozilla.org/en-US/collusion/ (last visited July 11, 2012).
[38] *See* 15 U.S.C. § 1681g.
[39] WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL ECONOMY, (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf
[40] 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.
[41] 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.

consumers in the management of their personal information. Similar provision are found also un US law in, for example, the data destruction provision of the Video Privacy Protection Act of 1988.[42] This issue was not addressed at the workshop, nevertheless, EPIC believes that it is an important part of any recommendations the Commission might adopt.

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

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. Despite EPIC's recommendations, the workshop failed to confront this issue. Notice, by itself, does not 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."[43] 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. Similarly, the workshop did not discuss any remedy or adjustment to mobile privacy practices. 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."[44]

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:

[42] Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(e) (2006).
[43] Statement of Rights and Responsibilities Update, FACEBOOK, https://www.facebook.com/note.php?note_id=10151420037600301 (last visited July 11, 2012).
[44] *Id.* (comments of Abine, Inc.).

> (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
> (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.[45]

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.[46] The Council of Europe Convention 108 contains principles regarding data quality, sensitive data categories, data security, and transborder data flows.[47] 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.[48] Accordingly, EPIC recommends that The Commission address the connection between disclosure and a broader regime of privacy protection. Notice should be a part of a broader regime that incorporates substantive privacy protections for consumers. Specifically, The Commission should consider how best to establish substantive privacy protections for mobile services.

[45] Privacy Act of 1974, 5 USC § 552a.
[46] 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.
[47] 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.
[48] WHITE HOUSE, *supra* note 39.

Too often, "notice" operates as a waiver or disclaimer to the disadvantage of users of Internet-based services. By simply stating, in vague terms, how a company might use the data it acquires users are left with a "take it or leave it" proposition: if they do business with the firm, they have agreed to all the ways the firms intends to use their data. If they object to the uses, they must go elsewhere. This is not a policy that favors privacy protection. The Federal Trade Commission has an obligation to safeguard consumers in the new digital marketplace and that requires developing standards that are meaningful and enforceable.

V. Conclusion

EPIC reiterates its preference for substantive privacy protections over procedural guidelines and urges the Commission to focus on applying Fair Information Practices to the mobile environment. To the extent the Commission is focused on disclosure, EPIC recommends broadening its conception of disclosure to include principles of transparency and access and correction.

Respectfully Submitted,

Marc Rotenberg, EPIC Executive Director
David Jacobs, EPIC Consumer Protection Fellow
Allegra Funsten, EPIC IPIOP Clerk
John Sadlik, EPIC IPIOP Clerk
Electronic Privacy Information Center
1718 Connecticut Ave. NW Suite 200
Washington, DC 20009
202-483-1140 (tel)
202-483-1248 (fax)