COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

To

THE NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

Of the

DEPARTMENT OF COMMERCE

Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct

RIN 0660–XA27

"Docket No. 120214135-2135-01"

April 2, 2012

By notice published on March 5, 2012, the National Telecommunications and Information Administration ("NTIA") has requested comment on "substantive consumer data privacy issues that warrant the development of legally enforceable codes of conduct, as well as procedures to foster the development of these codes."[1] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments and recommendations to ensure that the Consumer Privacy Bill of Rights is given legal force, either by an agency rule or by legislation.

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 federal agencies such as 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

[1] Multistakeholder Process To Develop Consumer Data Privacy Codes of Conduct, 77 Fed. Reg. 13098 (proposed Mar. 5, 2012), http://www.ntia.doc.gov/files/ntia/publications/fr_privacy_rfc_notice_03052012_0.pdf.

and to safeguard the privacy rights of consumers.[2] EPIC's 2010 complaint concerning Google Buzz provided the basis for the Commission's investigation and October 24, 2011 subsequent settlement concerning the social networking service.[3] In that case, the Commission found that Google "used deceptive tactics and violated its own privacy promises to consumers when it launched [Buzz]."[4] EPIC's FTC complaints were also responsible for the Commission's recent settlement with Facebook.[5] Furthermore, EPIC has previously recommended comprehensive privacy standards for NTIA privacy working groups.[6]

EPIC supports the principles outlined by the White House in the Consumer Privacy Bill of Rights ("CPBR"). The release of the report, and the strong statement in favor of privacy by President Obama, were important first steps toward safeguarding the digital privacy of consumers. However, the privacy principles in the CPBR must be meaningfully implemented and enforced. EPIC recommends that the agency ensure transparency, inclusiveness, and judicial review by implementing the CPBR through the Administrative Procedure Act. Furthermore, EPIC urges the agency to refine the current CPBR and to continue to develop additional privacy

[2] *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.

[3] Press Release, Federal 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.").

[4] *Id.*

[5] Facebook, Inc., (2009) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf [hereinafter EPIC 2009 Facebook Complaint]; Facebook, Inc., (2010) (EPIC Supplemental Materials in Support of Pending Complaint and Request for Injunction, Request for Investigation and for Other Relief) [hereinafter EPIC 2009 Facebook Supplement]; Facebook, Inc., (2010) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief) , https://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf [hereinafter EPIC 2010 Facebook Complaint].

[6] *See* EPIC, Privacy Guidelines for the National Information Infrastructure: A Review of the Proposed Principles of the Privacy Working Group, 1994, https://epic.org/privacy/internet/EPIC_NII_privacy.txt.

principles. Finally, EPIC recommends that the CPBR be ultimately codified through comprehensive privacy legislation.

I. The Consumer Privacy Bill of Rights

Building on the recommendations of a Green Paper on Privacy and Innovation released by the Department of Commerce's Internet Policy Task Force in December 2010, the Administration released Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy.[7] The report contains a Consumer Privacy Bill of Rights with the following principles:

- Individual Control: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.
- Transparency: Consumers have a right to easily understandable and accessible information about privacy and security practices.
- Respect for Context: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
- Security: Consumers have a right to secure and responsible handling of personal data.
- Access and Accuracy: Consumers have 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.
- Focused Collection: Consumers have a right to reasonable limits on the personal data that companies collect and retain.
- Accountability: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.[8]

The Consumer Privacy Bill of Rights discusses several high-profile privacy issues, including online advertising, data brokers, and children's privacy. The report encourages online

[7] 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 [hereinafter White House, CPBR].
[8] *Id.* at 1.

advertising companies to "refrain from collecting, using, or disclosing personal data that may be used to make decisions regarding employment, credit, and insurance eligibility" and cited a "Do Not Track" mechanism as an example of a beneficial privacy-enhancing technology.[9] The report calls on data brokers to "seek innovative ways to provide consumers with effective Individual Control."[10] Finally, the report notes that "the principles in the Consumer Privacy Bill of Rights may require greater protections for personal data obtained from children and teenagers than for adults."[11]

II. NTIA's Request for Public Comment

NTIA seeks comment on two issues: the issues that should be addressed through the privacy multistakeholder process, and the manner in which the multistakeholder process should be implemented.[12] Specifically, NTIA suggests an initial process to facilitate the implementation of the Transparency principle in mobile app privacy notices.[13] NTIA also identifies open participation and the concept of consensus as two primary procedural issues to address.[14]

III. Previous Efforts that have Emphasized Self-Regulation and Voluntary Adherence Have Failed to Protect Consumers

NTIA asks:

> 13. Are there lessons from existing consensus-based, multistakeholder processes in the realms of Internet policy or technical standard-setting that could be applied to the privacy multistakeholder process? If so, what are they? How do they apply?
>
> 15. Are there multistakeholder efforts that have failed to achieve consensus? Why do these efforts fail to reach consensus? What policies or standards, if any, resulted from these efforts?[15]

---

[9] *Id.* at 12.
[10] *Id.* at 13.
[11] *Id.* at 15.
[12] *See* Multistakeholder Process To Develop Consumer Data Privacy Codes of Conduct, 77 Fed. Reg. 13098 (proposed Mar. 5, 2012), http://www.ntia.doc.gov/files/ntia/publications/fr_privacy_rfc_notice_03052012_0.pdf.
[13] *Id.*
[14] *Id.*
[15] *Id.* at 13100.

EPIC shares the concerns raised by other organizations over the effectiveness of voluntary, self-regulatory regimes. In numerous instances, voluntary multistakeholder processes have failed in the absence of regulation. The World Privacy Forum ("WPF") conducted a recent study on various privacy self-regulatory, multistakeholder processes.[16] The research analyzed "industry-supported self-regulatory programs for privacy," "government privacy self-regulatory activities," and joint industry-government self-regulatory efforts.[17]

WPF concluded that "the majority of the industry self-regulatory programs that were initiated failed in one or more substantive ways, and, many disappeared entirely."[18] In its discussion about why industry-supported self-regulatory programs failed, WPF discussed various privacy self-regulatory efforts, including the Privacy Leadership Initiative, the Online Privacy Alliance, and the BBBOnline Privacy Program.[19] The report's findings highlighted three important areas on which NTIA should focus when implementing the stakeholder process: (1) technology neutral codes of conduct; (2) transparency in the stakeholder process; and (3) regulatory enforcement.

The WPF report found that "[t]he standards promulgated by the self-regulatory programs were often general and quickly became outdated because of technology and other changes."[20] Therefore, it is essential that the codes of conduct are applicable to ever-evolving technology and the corresponding privacy implications affecting consumer data privacy.

Additionally, the WPF report acknowledges the difficulty in finding original documentation detailing the work and progress of previous privacy self-regulatory bodies.[21]

---

[16] Robert Gellman & Pam Dixon, *Many Failures: A Brief History of Privacy Self-Regulation in the United States*, World Privacy Forum (2011), *available at* http://www.worldprivacyforum.org/pdf/WPFselfregulationhistory.pdf.
[17] *Id*. at 7-8.
[18] *Id*. at 2.
[19] *Id*. at 7.
[20] *Id*. at 9.
[21] *Id*.

NTIA has stated, "[p]roviding timely, relevant information in an accessible manner is crucial to effective transparency."[22] To ensure transparency, the stakeholders should memorialize their decision making process, and any reports and research on which they will rely.

The WPF report also strongly emphasizes the need for regulatory enforcement. A 2010 WPF report analyzed the US-EU Safe Harbor Framework, a government supervised industry self-regulatory process, which, like the NTIA multistakeholder process, was governed by the Department of Commerce.[23] The Safe Harbor Framework provided guidelines for personally identifiable information exported from Europe to the United States. The 2010 WPF report found that "[u]nlike most other privacy self-regulatory efforts the Safe Harbor Framework continues to exist, largely because of the government role."[24] Lack of genuine enforcement mechanisms both attracted industry participation and also decreased industry compliance. Industry was inclined to participate in the Safe Harbor Framework to further facilitate commercial transactions with EU Member States. However, because the Safe Harbor Framework has not been enforced, "evidence . . . suggests that the number of companies not in compliance [with the Framework] has increased over time."[25]

IV. The Administration Should Conduct a Public Rulemaking Pursuant to the Administrative Procedure Act

EPIC believes that the procedures established in the public rulemaking process, pursuant to the Administrative Procedure Act ("APA") (5 U.S.C. § 500 *et seq*.), would be more effective in implementing the CBPR and corresponding codes of conduct. The APA is a more durable and more well established process than "mutlistakeholderism" for a public agency to receive public

[22] 77 Fed. Reg.13100.
[23] World Privacy Forum, *The US Department of Commerce and International Privacy Activities: Indifference and Neglect* (2010), *available at* http://www.worldprivacyforum.org/pdf/USDepartmentofCommerceReportfs.pdf.
[24] *Many Failures: A Brief History of Privacy Self-Regulation in the United States*, 4.
[25] *Id*. at 21.

comments on agency action. The APA notice and comment rulemaking process[26], creates meaningful, transparent, and inclusive public participation in agency regulations. Public rulemaking will permit all interested persons, including those without access to Washington-based meetings, to express their views. It will also impose time limits and requirements on the agency that will help ensure that public comments are fully considered and that public participation is meaningful.

After agencies have considered public comments and adopted final regulations, final agency action is subject to judicial review.[27] This helps ensure that whatever action is taken by the agency reflects an outcome that is consistent with purpose of the rulemaking and the comments received. In the absence of judicial review, the agency will allow itself extraordinary discretion in determining the purposes of the exercise, the weight of the comments, and even when to conclude the process.

V. The Administration Should Continue to Refine and Develop the CPBR

At minimum, the process should result in the implementation of the entire CPBR. However, the CPBR is not an exhaustive list of privacy practices. Accordingly, EPIC urges the Administration to continue to expand on and update the CPBR. Other executive bodies that have proposed new privacy protections have updated earlier privacy frameworks in light of changing technologies and business practices. Thus, the European Commission's proposed reforms of the 1995 data protection rules[28] do not restate old principles, but update and modernize the principles to guarantee privacy rights in the future.[29] Similarly, the CPBR should not merely restate Fair

[26] Administrative Procedure Act, Pub.L. 79-404, codified at 5 U.S.C. § 553
[27] *Id.* §706.
[28] Council Directive 95/46, art. 12, (EC), http://www.dataprotection.ie/viewdoc.asp?docid=93.
[29] *See* European Comm'n, *Commission proposes a comprehensive reform of the data protection rules* (Jan. 25, 2012), http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

Information Practices from the Privacy Act of 1974.[30] There are many national and international privacy protections that either provide further clarification on the CPBR principles or contain additional practices not listed in the CPBR. For example, the American Society for Information Science (ASIS) Code of Ethics for Information Professionals requires members to "minimiz[e] data collected about clients, patrons, or users" to "treat fairly all persons regardless of race, religion, sex, sexual orientation, age, or national origin."[31] 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. [32] Privacy Enhancing Technologies and Privacy by Design should also be incorporated in the recommendations of the agency. EPIC encourages the Administration to refine the current CPBR principles and to continue to develop additional privacy practices.

Because the CPBR is not an exhaustive set of privacy practices, the topics around which the multistakeholder process operates should not be limited to those contemplated in the Administration's White Paper. The Administration recognizes that "[t]his list is not exhaustive," and "welcomes comments on any of these topics as well as descriptions of other topics that commenters would like NTIA to consider for the privacy multistakeholder process."[33] Additional topics that should be examined include facial recognition and facial detection software, anonymization, the implementation of privacy by design, and surveillance and data processing by Internet Service Providers.

---

[30] Privacy Act of 1974, 5 USC § 552a.
[31] Code of Ethics for Info. Professionals, Am. Soc'y for Info. Science (1992).
[32] 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/Commun/QueVoulezVous.asp?NT=108&CM=12&DF=25/01/2010&CL=ENG
[33] http://www.ntia.doc.gov/files/ntia/publications/fr_privacy_rfc_notice_03052012_0.pdf 13100

III. The CPBR Should be Enacted Through Comprehensive Privacy Legislation

EPIC recommends that the CPBR be enacted through comprehensive privacy legislation. As explained above, voluntary, self-regulatory approaches have failed to protect consumers. Because the Codes of Conduct produced by the multistakeholder process are not binding unless they are voluntarily adopted, companies will be free to ignore the Codes of Conduct. Thus, without legislation, the multistakeholder process could suffer from many of the same flaws as other voluntary approaches. EPIC recommends that the Administration augment the legislative process by developing its own draft bill containing the CPBR, and by providing a formal process for streamlined communication with Congress as developments in the multistakeholder process occur.

Indeed, the Administration itself recognizes the importance of legislation. In announcing the White Paper, President Obama stated that "My Administration will work to advance these principles and work with Congress to put them into law."[34] Part IV of the Administration's White Paper "urges Congress to pass legislation adopting the Consumer Privacy Bill of Rights."[35] The Administration recommends legislation that would grant both the FTC and State Attorneys General the authority to enforce each element of the CPBR.[36] The FTC would also be given authority under the Administrative Procedure Act to issue rules that establish a process for reviewing codes of conduct and ensuring that they fairly implement the CPBR.[37] The Administration also recommends a safe harbor mechanism under which companies could follow a code of conduct that the FTC has reviewed and approved.[38]Although State Attorneys General would have authority to enforce the CPBR, the CPBR would preempt more protective state

[34] White House, CPBR.
[35] *Id.* at 35.
[36] *Id.* at 36.
[37] *Id.* at 37.
[38] *Id.*

legislation.[39] Finally, the Administration recommends creating a national standard for notification in the event of a data breach.[40]

The legislative framework called for by the Administration could be improved by granting consumers a private right of action and allowing states the freedom to pass more protective privacy laws. Private rights of action strengthen enforcement and allow individuals to seek remedies. Additionally, because it is often difficult to place a dollar value on data breaches and privacy infringements, it is important that any private right of action also include a statutory damages provision. This would empower consumers to enforce the law themselves and create a strong disincentive for the irresponsible handling of consumer data. Not only would this provide the opportunity for individuals who have been harmed by security breaches to have their day in court, it would also provide a necessary backstop to the current enforcement scheme, which relies almost entirely on the Federal Trade Commission, acting on its own discretion and without any form of judicial review, to enforce private rights. For these reasons, many state laws include private rights of action. California, Hawaii, Louisiana, and Washington, for instance, include provisions in their state data breach laws that allow consumers to bring a civil action and recover damages.[41]

The Administration's suggestion that the enacted CPBR preempt conflicting state laws would potentially nullify more effective state legislation and foreclose future legislative innovation at the state level. Privacy laws have typically created a federal baseline and allowed the states to adopt more stringent safeguards if they wish. This approach to consumer protection is based upon principles of federalism that allow the states to experiment with new legislative

[39] *Id.*
[40] *Id.*
[41] Cal. Civ, Code § 1798.82 (2011), Haw. Rev. Stat. § 487N-2 (2011), La. Rev. Stat. § 51:3071 *et seq*. (2011), Wash. Rev. Code § 19.255.010, 42, 56, 590 (2011).

approaches to emerging issues. Because states enjoy a unique perspective that allows them to craft innovative programs to protect consumers, they should be permitted to continue to operate as "laboratories of democracy" in the privacy and data security arena. State legislatures are closer to their constituents and the entities they regulate; they are the first to see trends and problems, and are well-suited to address new challenges and opportunities that arise from evolving technologies and business practices. This is why privacy bills have typically created a federal baseline and allowed the states to adopt more stringent safeguards if they wish.

Finally, the Administration's concern for flexible solutions weighs against preempting state legislation. Privacy problems are rapidly changing and the states need the ability to respond as new challenges emerge. California, for example, has recently updated its data breach notification law to specify the information that should be provided by data holders to individuals in the event of a breach and to require that the state Attorney General be notified in the event of a large breach.[42] Massachusetts is also considered updates to its data breach law in response to new threats.[43] It is very likely that the states will continue to face new challenges in this field. Thus, the temptation to establish a national standard for breach notification should be resisted, particularly given the rapidly changing nature of the problem.

In the interim, the Administration could undertake several measures to facilitate the development of legislation. First, the Administration could draft a proposed bill codifying the CPBR. Doing so would clarify the scope of the principles as the Administration sees them and provide concrete language to which stakeholders can react. Second, the Administration could

[42] *See* EPIC, California Passes Updated Data Breach Legislation, http://epic.org/2011/09/california-passes-updated-data.html (last visited September 11, 2011).
[43] Jason Gavejian, *California and Massachusetts Legislatures Push Data Breach and Security Bills*, Workplace Privacy, Data Management, and Security Report (May 3, 2011), http://www.workplaceprivacyreport.com/2011/05/articles/workplace-privacy/california-and-massachusetts-legislatures-push-data-breach-and-security-bills/.

establish a formal mechanism for communication with Congress throughout the multistakeholder process. As Codes of Conduct are developed, or as suggestions are made, this communication channel would provide expedited feedback to members of Congress ultimately responsible for drafting the bill.

VI. Conclusion

EPIC supports the principles contained in the CPBR. However, in order to achieve meaningful privacy protection for American consumers, EPIC urges the Administration to refine and develop the CPBR, follow the public rulemaking procedures set forth in the APA, and codify the CPBR in legislation.

Respectfully Submitted,

Marc Rotenberg, EPIC Executive Director
David Jacobs, EPIC Consumer Protection Fellow
Khaliah Barnes, EPIC Open Government Fellow
Electronic Privacy Information Center
1718 Connecticut Ave. NW Suite 200
Washington, DC 20009
202-483-1140 (tel)
202-483-1248 (fax)