



April 2, 2012

Lawrence Strickling
Assistant Secretary of Commerce for Communications and Information
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Washington DC, 20230
E-Mail: privacyrfc2012@ntia.doc.gov

AMERICAN CIVIL
LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

Re: Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct, RIN 0660-XA27

Dear Mr. Strickling:

The American Civil Liberties Union (ACLU)¹ appreciates the steps the Administration has taken in describing a consumer privacy bill of rights in its recent report *Consumer Data Privacy in a Networked World* and publishing its notice of inquiry to begin to convert those principles into enforceable codes of conduct and eventually full statutory protections.² However, in order for the multistakeholder process to be meaningful in developing enforceable provisions that truly protect consumers, the ACLU believes the National Telecommunications and Information Administration (NTIA) must (i) formally involve Congress in every step of the process and (ii) adopt full and fair procedures for stakeholder involvement. The ACLU also recommends four areas – mobile applications, government access to information, data retention limits, and facial recognition – where we believe the multistakeholder process could quickly achieve meaningful results for consumers.

LAURA W. MURPHY
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

ROBERT REMAR
TREASURER

¹ The ACLU is America's oldest and largest civil liberties organization, having more than half a million members, countless additional supporters and activists, and 53 affiliates nationwide. We advocate against unnecessary government intrusion into the lives of Americans and undue burdens on their privacy rights.

² *Consumer Data Privacy in a Networked World: A Framework of Protecting Privacy and Promoting Innovation in the Global Digital Economy*. Washington: Government Printing Office, Feb 2012; Request for Public Comment. National Telecommunications and Information Administration, *Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct*, 77 Fed. Reg. 13098 (March 5 2012).

I. Congressional Involvement

In the recent White House report on consumer data privacy which forms the basis for this notice, President Obama made a key commitment. After describing the rights necessary to protect consumer privacy, the President stated “My Administration will work to advance these principles and work with Congress to put them into law.” This commitment must remain the central focus of any process for creating standards for internet privacy.

The report envisions an initial process of developing codes of conduct, binding on companies that commit to them and enforceable through the Federal Trade Commission’s (FTC) authority to punish commercial entities that describe their conduct in an unfair or deceptive manner. However, these codes will never be enough on their own. Companies cannot bind their competitors, and industries that refuse to participate in the process can take themselves completely outside the authority of the FTC. Nor will companies have sufficient incentive to negotiate strong, effective practices without the threat of legislation.

It is incumbent upon the Administration and NTIA to take concrete steps within the multistakeholder process to realize the President’s stated desire to work with Congress to enact a new privacy statute. Specifically, the Administration and NTIA must:

- Formally invite members of Congress and their staff to take part in the process either as observers or participants;
- Adhere to a fixed timeline for notifying relevant committees and leadership in both the House and the Senate of the nature and progress of the deliberations of the process;
- Request Congressional hearings on issues of relevance to the process that require additional factual support and could benefit from Congressional investigation; and
- Draft language to convert the consumer privacy bill of rights into legislation suitable for action by Congress and, because the process addresses individual issues, craft language for Congress to consider in legislating on those issues.

Congress must be an active and engaged partner if the goals outlined by the Administration, including a robust consumer bill of rights, are to become reality. NTIA and the Administration must take formal measures to recognize the importance of Congress, establish procedures to solicit Congressional input, and communicate the progress of the multistakeholder process.

II. Procedure for Participation in the Multistakeholder Process

Establishing fair and open procedures for participation and decision-making within the multistakeholder process is critical to its success. Rules and procedures must be the first item on the agenda. Somewhat unfortunately, this Notice of Inquiry actually reverses that order. It first asks about what issue the process should consider and then asks for the process for consideration. This is precisely backwards. Stakeholders in a multistakeholder process must first decide how they will proceed and then use that process to determine what concrete measures they want to act upon together. This order will grant legitimacy to whatever subject is chosen and assure that the

stakeholders are addressing the problems that they determine are most important to their interests.

In Section III of this letter, we describe key policy issues that we believe would benefit from the involvement of a multistakeholder process. But that list merely represents the view of one stakeholder. Neither the NTIA nor any other entity can simply announce the topics for review by the process. Instead, for them to have legitimacy, the topics must arise from an agreement of the participants.

The ACLU and other consumer protection and privacy organizations have developed a joint set of standards to guide any multistakeholder process. These standards and the signatories to them are attached as an appendix to this document. They form a fair, transparent and reasonable basis for discussion. They must be adopted, along with other measures supported by different stakeholders, in order to allow action on any substantive consumer privacy issues.

III. Potential Topics for Discussion in a Multistakeholder Process

A multistakeholder process could fruitfully address at least four substantive issues germane to a discussion of consumer data privacy:

- A. Mobile applications;
- B. Notice of government access to electronic information held by third parties;
- C. Data retention limits on search terms; and
- D. Facial recognition.

A. Mobile applications

The regulatory notice identifies two criteria for determining what subject the multistakeholder process should pursue. Specifically, it envisions “an area where consumers and businesses will receive the greatest benefit in a reasonable timeframe.” These criteria are reasonable: everyone wants to maximize benefit for stakeholders, and no one wants an indefinite process. However, some of the suggested options NTIA has suggested for negotiation would not provide enough benefit to justify the effort necessary to achieve them.

For example, the proposal that the notice describes in the most detail, providing transparency for mobile applications, suffers from this deficiency. Consumer experience over the last 15 years has established that pop-up on-screen privacy policies are inadequate to protect privacy. Almost universally ignored by users, they are background noise that does not help consumers safeguard data. The Administration report on privacy, including its consumer bill of rights, is at its heart a rejection of this type of notice and choice policy. The Administration position recognizes that consumers need a full range of privacy tools, including not just transparency, but also limits on data use and transfer, control, security, access and accountability. A process convened with the expectation of achieving comprehensive privacy protections (either through codes of conduct or legislation) is doomed to failure if it then starts with goals that are both time-consuming and so modest as to be almost inconsequential.

However, while a focus on transparency of mobile app focus is too limited, a broader consideration of all the privacy issues created by mobile apps would be significant. In recent months, a wide range of privacy problems have arisen from mobile applications. Those controlling a number of apps have admitted to downloading user contact information without consent. Others have downloaded data on users, like location, age, and other personal information. According to a recent survey, only about 5% of apps have a privacy policy.³ Given these facts, we believe there would be significant value in applying all of the principles from the consumer privacy bill of rights to mobile applications.

Apps are still a new enough technology that they can quickly incorporate new privacy requirements without disrupting either their own business models or forcing broad changes across the internet. Also because they tend to be distributed through just a few channels--mobile app stores--those channels are well positioned to require them to adopt best practices.

Given the lack of consistent and enforceable privacy standards, the application of privacy protections to mobile app technology would benefit consumers immediately and directly. It would also increase user confidence in such applications, allowing an industry that has burgeoned in recent years to continue to thrive. Resolving issues in the mobile space, such as the appropriateness of third party data sharing and limits for retaining data, may have the important additional benefit of helping to reach consensus on appropriate controls for broader uses of information.

B. Notice of government access to electronic information held by third parties

As a result of widespread use of the internet and cloud computing, many documents, transactional records, and correspondence are no longer held by an individual on a personal hard drive, but instead are held by third-party companies. A steady erosion of a citizen's personal privacy in government investigations has resulted from this change. Before the advent of the internet, government investigators would have to obtain letters, business records, and other information of interest directly from the individual. Consequently, citizens had notice of a government investigation and the opportunity to challenge the breadth of a subpoena or other order. Now records are frequently gathered from a third party, with and without notice to the affected individual.⁴

Changing technology has precipitated two distinct privacy problems relating to notice. First, if a company does not notify an individual of a subpoena or other order, the user cannot challenge the scope of the invasion of their personal privacy. Some companies have been proactive in notifying their users of these investigations. One of the most notable companies in this regard is Twitter, which has notified individuals about pending investigations surrounding

³ Rafe Needleman. "Path CEO: We are sorry, and we've deleted your address book data." *CNET*, Feb. 8 2012; Scott Thurm and Yukari Iwatani Kane. "Your Apps Are Watching You." *The Wall Street Journal*, Dec. 17 2010; Cameron Scott. "In CA Mobile App Stores to Require, Disclose Privacy Policies." *PC World*, Feb 22 2012.

⁴ Exacerbating this problem, protections against government access to electronic information, including when notice should be provided, have not been substantially updated since 1986. 18 U.S.C. 2701 et al.

the Occupy Wall Street protests, Wikileaks investigation, and criticism of the Pennsylvania Attorney General.⁵

Lack of notice by companies also results in a lack of awareness of the problem in the aggregate. Citizens cannot properly evaluate and regulate the actions of government if they never receive information about government practices. Google has been a leader in providing transparency in this regard. Since July 2009, every six months it has published an aggregate description of the types and total number of orders it receives.⁶ This voluntary process has been one of the few ways that the public has gained any insight into the breadth and growth of these types of orders.

As Twitter and Google's actions demonstrate, both these transparency measures are feasible and would result in significant net privacy gains for consumers. The multistakeholder process would be a fruitful place to discuss how those companies developed their policies, what barriers might exist to more widespread adoption, and how to codify best practices.

C. Data retention limits on search terms

Companies cannot share information they do not retain. This axiomatic privacy principle is a crucial, practical check against a number of privacy harms, including identity theft and other improper uses of data. Strict data retention standards also benefit companies, limiting the severity and breadth of data breaches and the ensuing liability from harm. The consumer privacy bill of rights describes this principle as focused collection; "Companies should securely dispose of or de-identify personal data once they no longer need it".

Data retention limits can be difficult to enshrine in practice. Different applications and industries need data for different purposes and retain it for different periods of time. Setting a single retention limit across the web would not be effective and would likely be both over- and under-prescriptive. However, building on industry best practices should allow for the development of retention limits for particular classes of data. Such a framework would also fit squarely within the stated goal of the process to "conduct a privacy multistakeholder process focused on a definable area where consumers and businesses will receive the greatest benefit in a reasonable period of time."⁷

Data retention limits for search terms are one specific class of information that could be usefully addressed as part of a multistakeholder process. Search queries tend to be very detailed and provide intimate portraits of individual lives, revealing extensive details about work and personal life. In 2006, AOL released three months of anonymized search information on

⁵ Noam Cohen. "Twitter Shines a Spotlight on Secret F.B.I. Subpoenas." *The New York Times*, Jan 9 2011; Quinn Norton. "Boston D.A. Subpoenas Twitter Over Occupy Boston, Anonymous." *Wired*, Dec 30 2011; David Kravets. "Pennsylvania AG Dropping Twitter Subpoena" *Wired*, May 21 2010.

⁶ See <http://www.google.com/transparencyreport/governmentrequests/map/> Note this map only includes orders Google is not barred by law from sharing. Some types of government orders such as National Security Letters contain mandatory bans on disclosure.

⁷ Request for Comment, 77 Fed. Reg. 13098 at 13099.

657,000 users in an effort to assist researchers.⁸ The company quickly removed the information after reporters were able to use the anonymized terms to identify particular users, including Thelma Arnold, a 62-year old widow who lives in Lilburn, Georgia. The details from the search terms powerfully demonstrate the impact the revelation of these terms can have on individual privacy.

From the *New York Times*:

In the privacy of her four-bedroom home, Ms. Arnold searched for the answers to scores of life's questions, big and small. How could she buy "school supplies for Iraq children"? What is the "safest place to live"? What is "the best season to visit Italy"?

Her searches are a catalog of intentions, curiosity, anxieties and quotidian questions. There was the day in May, for example, when she typed in "termites," then "tea for good health" then "mature living," all within a few hours.

Her queries mirror millions of those captured in AOL's database, which reveal the concerns of expectant mothers, cancer patients, college students and music lovers. User No. 2178 searches for "foods to avoid when breast feeding." No. 3482401 seeks guidance on "calorie counting." No. 3483689 searches for the songs "Time After Time" and "Wind Beneath My Wings."

At times, the searches appear to betray intimate emotions and personal dilemmas. No. 3505202 asks about "depression and medical leave." No. 7268042 types "fear that spouse contemplating cheating."⁹

Given the potential impact that the release of search terms would have on consumers and given the limited number of companies providing web search services, creating data retention limits for search terms is an important topic for negotiation, limited in scope but with the potential to provide significant benefit to consumers.¹⁰

D. Facial Recognition

In the past, photographs and video footage enjoyed a significant level of practical anonymity. Unless a picture was captioned with the subjects name or other information, it was not identifiable by a machine and could not be linked to a broader profile of the individual. Facial recognition technology has the capacity to change that. By identifying individuals, face recognition creates a broad new category of information which can powerfully document individual lives and reveal other types of personal information.

⁸ Michael Barbaro and Tom Zeller Jr. "A Face Is Exposed for AOL Searcher No. 4417749." *The New York Times*, August 9 2006.

⁹ *Id.*

¹⁰ Three companies, Google, Microsoft and Yahoo, account for 95.5% of searches in the United States. comScore. (2012). comScore Releases February 2012 U.S. Search Engine Rankings [Press release]. Retrieved from: http://www.comscore.com/Press_Events/Press_Releases/2012/3/comScore_Releases_February_2012_U.S._Search_Engine_Rankings

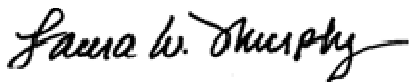
Researchers at Carnegie Mellon University, led by Professor Alessandro Acquisti, were able to use commercially available facial recognition software to match mobile phone photos of people to individual Facebook photos and profiles.¹¹ In addition to names, such profiles sometimes included a host of other personal information, sometimes enough to guess information like Social Security numbers. In describing this research, Acquisti said, “Your face is a conduit between the online and offline world. Soon, anyone may run face recognition anywhere. It raises the issue of what privacy will mean.”¹²

Facial recognition is a new technology, one that has not been regulated by the government in the United States or subject to industry codes of conduct. One possible regulatory approach is to develop codes of conduct around the collection of a facial image match. Such a match would be the mathematical pattern of shapes and points derived from a human face used to identify a particular individual. Once a company develops this match for a particular individual, that match would then be treated like personally identifying information, such as a Social Security number, which could be regulated using the existing fair information practice principles embodied in the consumer privacy bill of rights.

IV. Conclusion

Formal Congressional involvement and a fair, open, and robust process are key procedural protections for any multistakeholder process. Without both, the process will lack both legitimacy and the practical elements necessary for success. Once adequate procedural protections have been adopted, we urge that the multistakeholder process engage in four areas – mobile applications, government access to information, data retention limits, and facial recognition – all of which can be resolved in a reasonable timeframe while providing meaningful protections for consumers.

Sincerely,



Laura W. Murphy
Director, Washington Legislative Office



Christopher Calabrese
Legislative Counsel

¹¹ David Goldman. “Your face on Facebook is key to personal info.” *CNN Money*, August 5 2011.

¹² *Id.*

Appendix

Principles for Multi-Stakeholder Process

February 23, 2012

Civil society groups believe that protecting the online privacy of consumers is crucial to ensuring the availability, utility, and vitality of the Internet. For any approach to privacy to be meaningful, it must reflect fair information practices, including mechanisms to assure accountability. The US Department of Commerce is proposing a multi-stakeholder process for developing better applications of privacy principles. For the multi-stakeholder process to succeed, it must be representative of all stakeholders and must operate under procedures that are fair, transparent, and credible.

We believe the following baseline principles will provide the multi-stakeholder process the legitimacy it needs to succeed.

Principles:

1. No multi-stakeholder process can succeed unless consumer representation is robust and reasonably balanced. Only consumer representatives can determine who speaks for consumers.
2. To the greatest extent practicable, the multi-stakeholder process should occur in the open with public sessions and public documents. All substantial decisions must be made in open sessions.
3. Any stakeholder may submit proposals and those proposals must be addressed and resolved within the consensus process.
4. Participants, but not necessarily observers, must specifically identify their employer and/or the group, industry, or organization whose interest they represent.
5. There must be a fair opportunity for public engagement at all levels of the stakeholder process. Stakeholders must be allowed to communicate with members of their communities about the multi-stakeholder process in any way that the stakeholders see fit, including use of electronic processes such as web sites, social media, and other methods.
6. The formal publication of any consensus document or decision must include dissenting views and statements.
7. Decisions must be based on a fair and broad consensus among stakeholders rather than a majority vote by participants. The process should seek to resolve issues through open discussion, balance, mutual respect for different interests, and consensus.

8. A multi-stakeholder process needs to be fully informed by stakeholders from civil society. As such, in person meetings may only be scheduled if adequate resources are made available to facilitate in person participation by civil society. Otherwise, meetings may only be conducted electronically to facilitate equal participation by all stakeholders. Meeting locations must be chosen with robust input from civil society stakeholders.

9. All stakeholders must receive a copy of a draft document at least ten days prior to consideration or presentation of the document at any level of the stakeholder process.

10. At the end of 12 months or at any other time, civil society participants may decide to reevaluate the multi-stakeholder process and make recommendations for changes in rules, procedures, or process.

Signatories:

World Privacy Forum

American Civil Liberties Union

Center for Digital Democracy

Consumer Action

Consumer Federation of America

Consumers' Union

Consumer Watchdog

Electronic Frontier Foundation

National Consumers' League

Privacy Rights Clearinghouse

US PIRG

Document information:

Publication date: February 23, 2012

Authors: Signatory organizations

Permalink: <http://www.worldprivacyforum.org/pdf/MultiStakeholderPrinciples2012fs.pdf>