BEFORE THE
DEPARTMENT OF COMMERCE

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

Request for Public Comments

MULTISTAKEHOLDER PROCESS TO DEVELOP CONSUMER DATA PRIVACY CODES OF CONDUCT

DOCKET# 120214135-2203-02

COMMENTS OF THE FUTURE OF PRIVACY FORUM

Jules Polonetsky
Co-Chair and Director, Future of Privacy Forum
919 18th Street, NW Suite 901
Washington, DC 20036
202-713-9466
julespol@futureofprivacy.org

Christopher Wolf
Founder and Co-Chair, Future of Privacy Forum
Partner
HOGAN LOVELLS US LLP
555 13th Street, NW
Washington, DC 20004
202-637-8834
christopher.wolf@hoganlovells.com
Counsel for the FUTURE OF PRIVACY FORUM

April 2, 2012

I. INTRODUCTION

The Future of Privacy Forum ("FPF") respectfully submits these comments in response to the National Telecommunications and Information Administration's ("NTIA's") request for public comments ("Request for Comments") dated March 5, 2012.[1] The Request for Comments solicits feedback on substantive consumer privacy issues that warrant the development of legally enforceable codes of conduct, as well as procedures to foster the development of these codes. The Request for Comments follows the Administration's February 23, 2012 release of a report titled *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in a Global Digital Economy* (the "Privacy and Innovation Blueprint"). Two of the key elements of the Privacy and Innovation Blueprint are: (1) the "Consumer Privacy Bill of Rights"; and (2) a multistakeholder process ("MSHP") convened by NTIA to develop enforceable codes of conduct to implement the Consumer Privacy Bill of Rights.

FPF strongly supports the Administration's efforts to enhance data privacy protections and promote consumer trust in a networked society. FPF also supports NTIA's efforts to facilitate the development of enforceable codes of conduct through a MSHP. With the rapid evolution of technology, an approach in lieu of technology-specific and prescriptive legislation and one that allows affected parties to participate is prudent.

As discussed below, FPF suggests that a first area that the MSHP should address is mobile device applications ("apps"). The continued proliferation and use of mobile devices by consumers for a multitude of communication and computing purposes, with a corresponding

[1] *Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct*, Request for Public Comments, Department of Commerce, National Telecommunications and Information Administration, 77 Fed. Reg. 13,098 (Mar. 5, 2012) ("Request for Comments").

increase in downloads and use of mobile apps, makes app privacy a priority. Reports of privacy issues with mobile apps abound, making the issue timely and urgent.[2]

In proposing mobile apps as a first area of focus for the MSHP process, FPF notes at the outset the important work that has already been done in the area and we do not mean to suggest that parallel stakeholder efforts already started outside the NTIA-convened process should end. To the contrary, FPF urges the integration of the foundational work already done and the encouragement of parallel activities. For example, app best practices guidelines and model app privacy policies already have been produced by the GSMA (representing mobile operators), the Electronic Frontier Foundation ("EFF"), the Center for Democracy and Technology ("CDT"), FPF, and the Mobile Marketing Association ("MMA"), which provide a substantive starting point for the consideration of binding codes of conduct. Further progress is expected from efforts such as the April 25, 2012 app developer privacy summit convened by FPF, the Application Developers Alliance ("ADA"), and the Stanford Center for Information and Society.[3]

II. ABOUT THE FUTURE OF PRIVACY FORUM AND ITS EFFORTS TO DEVELOP IMPROVED PRIVACY AND DATA SECURITY PRACTICES

FPF is a Washington, DC-based think tank focused on advancing responsible data practices. FPF is led by privacy leaders Jules Polonetsky and Christopher Wolf and includes an advisory board comprised of leading figures from industry, academia, law and advocacy groups.[4]

---

[2] *See* Polonetsky and Wolf, *App developers, not regulators, are best suited to solve privacy problem*, MercuryNews.com (Mar. 19, 2012), *available at* http://www.mercurynews.com/opinion/ci_20209958/jules-polonetsky-and-christopher-wolf-app-developers-not.

[3] *See App Developer Privacy Summit*, http://cyberlaw.stanford.edu/events/app-developer-privacy-summit.

[4] The positions taken by FPF are entirely its own and do not necessarily reflect those of its supporters and advisory board members.

FPF hopes that its expertise with consumer privacy issues and in working with a broad array of stakeholders in the privacy community will make these comments useful to NTIA, and we briefly highlight some of our recent efforts here.

Among other important issues, FPF has worked to focus attention on the data collection issues raised by mobile apps. FPF believes that users should be provided with sufficient and timely information by app developers so that users can understand how data about them may be used when they interact with apps. To further this effort, FPF has created a resource center at www.applicationprivacy.org that contains emerging standards, best practices, privacy guidelines, platform and application store requirements, privacy policy generators, and self-assessment tools, as well as relevant laws and regulatory guidance, all of which can assist app developers in providing their users with appropriate privacy protections. In addition, FPF regularly conducts surveys of app privacy policies, including regular surveys that have documented how few apps have posted privacy policies.[5]

Another major FPF initiative concerns privacy and the smart grid. Modernization efforts are underway to make the current electrical grid "smarter" through the collection of data about consumer usage. FPF is a leader in this area, having convened the first smart grid privacy conference in Washington, DC. With the Privacy Commissioner of Ontario, FPF published a White Paper entitled *Smart Privacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation*.[6] FPF also operates a smart grid privacy resource center at

[5] *FPF Survey: Free Apps Better than Paid on Privacy Policies*, Future of Privacy Forum (Dec. 20, 2011), *available at* http://www.futureofprivacy.org/wp-content/uploads/FPF-Mobile-Apps-release.pdf.

[6] *Smart Privacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation*, Future of Privacy Forum; Information and Privacy Commissioner, Ontario, Canada (Nov. 2009), *available at* http://www.ipc.on.ca/images/resources/pbd-smartpriv-smartgrid.pdf.

www.smartgridprivacy.org and recently submitted comments on smart grid issues to the California and Colorado public utilities commissions.[7] As platforms supporting apps for the grid have recently launched, our efforts here are beginning to focus on responsible practice for these developers as well.

As the name suggests, FPF is focused on privacy issues that loom large for the future, which is why we are pleased to make this submission in connection with NTIA's and the Administration's focus on the future of consumer data privacy in the United States.

III. THE MULTISTAKEHOLDER PROCESS SHOULD FOCUS FIRST ON ADDRESSING CONCERNS OVER MOBILE APPS

The Request for Comments states that NTIA is "considering convening an initial [MSHP] to facilitate the implementation of the Transparency principle in the privacy notices for mobile device applications."[8] It also seeks comment on other potential topics, including "[o]ther issues associated with mobile apps in general (*e.g.*, a code of conduct that implements the full Consumer Privacy Bill of Rights)."[9] FPF strongly supports the creation of an MSHP focused on mobile app privacy issues.

---

[7] *See Comments of the Future of Privacy Forum on the Proposed Decision Adopting Rules to Protect the Privacy and Security of the Electricity Usage Data of the Customers of Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company* (June 2, 2011), *available at* http://www.futureofprivacy.org/wp-content/uploads/2011/06/FPF_Cal_PUC_Smar_%20Grid_Comments.pdf; *Comments of the Future of Privacy Forum, Proposed Rules Relating to Smart Grid Data Privacy for Electric Utilities*, 4 Code of Colorado Regulations 723-3 (Mar. 24, 2011), *available at* https://www.dora.state.co.us/pls/efi/efi_p2_v2_demo.show_document?p_dms_document_id=102498.

[8] Request for Comments at 13,099.

[9] *Id.*

Mobile apps have become a key part of everyday life for many Americans, and as the Request for Comments recognizes, they are "gaining in social and economic importance."[10] During the last week of 2011, more than 500 million mobile apps were downloaded in the United States.[11] Indeed, there now are more than a million apps and counting available to consumers. Those statistics alone show the app industry's breathtaking new role in how people use mobile technology. In fact, one recent TechNet study found that mobile apps are responsible for almost half a million jobs in the U.S. economy.[12]

Notwithstanding the skyrocketing growth of mobile apps, reports abound about severe flaws in how many apps treat their users' personal information. For example, there have been news reports of some apps uploading the contents of user address books without permission.[13] Others reports show that some apps copy entire photo libraries without specific user permission.[14] And most do not even include a basic privacy policy that informs users about the personal information that is being collected, used, and shared. One study estimates that 95% of apps do not include a privacy policy.[15] In light of these and other concerns, some legislators and

---

[10] *Id.*

[11] *Appy Holidays: The First Billion-Download Week,* All Things D (Jan. 2, 2012), *available at* http://allthingsd.com/20120102/appy-holidays-the-first-billion-download-week/ (discussing a report from Flurry Analytics).

[12] *Where the Jobs Are: The App Economy*, TechNet (Feb. 7, 2012), *available at* http://www.technet.org/wp-content/uploads/2012/02/TechNet-App-Economy-Jobs-Study.pdf.

[13] *See, e.g.*, *Mobile Apps Take Data Without Permission*, NY Times Bits Blog (Feb. 15, 2012), *available at* http://bits.blogs.nytimes.com/2012/02/15/google-and-mobile-apps-take-data-books-without-permission/.

[14] *See, e.g.*, *Apple Loophole Gives Developers Access to Photos*, NY Times Bits Blog (Feb. 28, 2012), *available at* http://bits.blogs.nytimes.com/2012/02/28/tk-ios-gives-developers-access-to-photos-videos-location/.

[15] *See Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications*, Press Release, California Department of Justice

consumer advocates have called for new laws and regulations for mobile apps, while the Federal Trade Commission ("FTC") recently encouraged companies providing mobile services to "work toward improved privacy protections."[16]

The privacy and security of user data is an important issue for the entire mobile app ecosystem. Users must trust mobile apps with their data or they will be more hesitant to download and use the services. App store/platform owners have an important role in promoting app privacy, and they are uniquely well-suited to increasing app developer awareness of privacy issues. App developers, in turn, need to continue educating themselves about the importance of protecting their users' privacy and data security. They should, for example, take advantage of the privacy tools already available to enhance their applications, such as those from PrivacyChoice, TRUSTe, FPF, and others. Device manufacturers and carriers also have an important role to play in protecting and enhancing user privacy. And all members of the mobile app ecosystem need to remember that accessing user data is a privilege, not a right. With mobile apps now supporting an estimated 500,000 jobs, too much is at stake to get it wrong. Privacy is a shared responsibility.

The MSHP model is especially well-suited to addressing key data privacy concerns in the mobile app ecosystem. For example, the various segments of the mobile app ecosystem, though continuing to evolve, are easily identifiable: app developers, advertising networks, content providers, app store/platform operators, equipment manufacturers, wireless service providers, and mobile device users. Thus, NTIA can determine the relevant, motivated stakeholders that

---

Office of the Attorney General (Feb. 22, 2012), *available at* http://oag.ca.gov/news/press_release?id=2630.

[16] *See, e.g., Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, Federal Trade Commission Report, 13, 73 (Mar. 2012), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

should be included in the MSHP. In addition, because the mobile app ecosystem is very decentralized, it is difficult for industry representatives to address concerns and develop self-regulatory solutions. Having a designated facilitator can help bring the parties together, as demonstrated by recent efforts from FPF and others described below.

The MSHP on mobile app privacy should focus initially on areas where progress has been limited due to the lack of cooperation or coordination among the companies in this ecosystem: transparency, notice, and choice. The Transparency principle is a key component of the Administration's Consumer Privacy Bill of Rights and industry best practices. In addition, the FTC has called for parties to develop "short, meaningful disclosures" and is exploring how such disclosures can be effective and accessible on small screens.[17] With respect to children's apps, the recent FTC report on children's app privacy disclosures found that many of the apps do not contain any data privacy disclosures.[18] Since the ability of apps to provide notice is in part dependent on the technical options permitted by platform operating systems, convening by NTIA will be invaluable in seeing this issue addressed.

Another critical transparency issue involves the tracking mechanisms used by apps, mobile ad networks, and analytics companies. Given the lack of cookies in the app ecosystem, apps and their partners have relied on device identifiers to provide their services. With one major platform beginning to prevent use of device identifiers, many apps are examining other equally or more sensitive tracking mechanisms. Apps that wish to adopt more privacy-friendly approaches are unable to easily do so without support for notice and choice mechanisms such as

[17] *See id.* at 13-14.

[18] *Mobile Apps for Kids: Current Privacy Disclosures Are Disappointing*, Federal Trade Commission Staff Report (Feb. 2012), *available at* http://ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.

those that the platforms have implemented for their own ad networks. Efforts by advocates or industry to coordinate discussions in this area have been fruitless. NTIA can play an essential role here in advancing efforts to ensure that options that support ad-supported apps and provide users with necessary controls are developed.

NTIA can build on the work done in these areas by FPF, CTIA-The Wireless Association®, GSMA, the Mobile Marketing Association, PrivacyChoice, TRUSTe, and other groups, as well as the FTC. In developing industry guidelines, the MSHP should also incorporate the Joint Statement of Principles entered into between major app platform providers and the California Attorney General.[19] By relying on these building blocks, NTIA can identify issues where agreement exists among the parties and then work to build on that agreement. After addressing mobile app transparency, NTIA should continue exploring the other elements of the Privacy Bill of Rights with respect to mobile apps and other networked services.

IV. THE NTIA PROCESS SHOULD SEEK TO ACHIEVE BROAD PARTICIPATION AND BUILD UPON PARALLEL STAKEHOLDER EFFORTS

FPF supports the proposed privacy MSHP and encourages NTIA to seek broad participation from all interested parties. However, while the official process to be convened by NTIA is indeed important – and constitutes one promising mechanism through which final agreements over codes of conduct should be reached – achieving consensus will also require both building on previous MSHPs (such as the industry efforts discussed above in Section III) as well as supporting ongoing current discussions such as the App Developer Privacy Summit that FPF and ADA will host on April 25, 2012.[20] There need to be parallel efforts in addition to the

[19] *See, e.g.*, Request for Comments at 13,099 nn.15, 16.

[20] *West Coast App Developer Privacy Summit*, Future of Privacy Forum, *available at* http://www.futureofprivacy.org/2012/02/16/west-coast-app-developer-privacy-summit/.

MSHP to educate stakeholders and begin to narrow the issues that the stakeholders will consider in developing codes of conduct.

The Department of Energy's ("Department's") efforts with respect to smart grid issues provide an illustrative example of how the MSHP can proceed effectively by integrating with ongoing stakeholder discussions. The Department recently convened a meeting of many of the stakeholders interested in ensuring responsible privacy rules for third-party access to smart grid data, including FPF.[21] Although this is an area where the states play a key role, companies using third-party data will, like many utilities, provide services across more than one state. By convening many of the interested parties, the Department advanced the exchange of information and promoted the discussion of key issues by many parties who were not previously aware of the full range of activity in this area. Key areas of future cooperation were identified, and discussions among a full range of stakeholders indicated a path for continued privacy advances. Efforts like these can play an important role in advancing the development of privacy practices, and NTIA should engage in and support such initiatives while also advancing the broader MSHP. Indeed, reports from the external discussions can be made during the MSHP and can help streamline and expedite those proceedings.

V. CONCLUSION

FPF fully supports the Administration's efforts to enhance data privacy protections and promote consumer trust in a networked society, including through an MSHP. Given the increasing role that mobile devices play in Americans' lives, the MSHP should first address mobile app privacy concerns. In addition, the MSHP should seek consensus through broad

[21] *See U.S. Department of Energy Smart Grid Privacy Workshop Summary Report*, SmartGrid.gov (Jan. 2012), *available at* http://www.smartgrid.gov/document/us_department_energy_smart_grid_privacy_workshop_summary_report.

participation and transparent discussions while recognizing and building upon parallel efforts being made by stakeholder groups outside the MSHP.

Respectfully submitted,

/s/ Jules Polonetsky

_____

Jules Polonetsky

Co-Chair and Director
Future of Privacy Forum
919 18th Street, NW Suite 901
Washington, DC 20006
(202) 713-9466
julespol@futureofprivacy.org

Christopher Wolf
Founder and Co-Chair
Future of Privacy Forum

Partner
HOGAN LOVELLS US LLP
555 13th Street, NW
Washington, DC 20004
202-637-8834
christopher.wolf@hoganlovells.com

Counsel for the
FUTURE OF PRIVACY FORUM

April 2, 2012