

Marlene Dortch, Secretary
Federal Communications Commission
445 12th St., S.W.
Washington, D.C. 20554

July 6, 2016

Re: WC Docket No. 16-106

Reply Comments in the matter of protecting the privacy of customers of broadband and other telecommunications services

Dear Ms. Dortch,

The undersigned organizations are submitting these reply comments to rebut arguments that the Federal Communications Commission (FCC) should defer to the National Telecommunications and Information Administration (NTIA) within the Department of Commerce to develop self-regulatory codes of conduct through a multistakeholder process to protect the privacy of broadband customers. We know firsthand the fallacy of these arguments because we have directly participated in some of the NTIA multistakeholder proceedings.

We believe that the FCC has the authority and the obligation to promulgate these rules, but setting that issue aside, it is clear to us that it would be impossible to reach consensus on protecting broadband customers' privacy through the NTIA multistakeholder process or any similar forum. There is no incentive for the relevant commercial interests to change their current business practices or align future practices to provide effective transparency, control, and security to broadband users absent a law or rules requiring them to do so. While best practices, voluntary codes of conduct, and recommendations made by government agencies and others can sometimes be helpful in encouraging good business practices, they are no substitute for enforceable rights.

History of the NTIA multistakeholder process

When the NTIA multistakeholder process was proposed in 2012¹ consumer and privacy groups suggested ten principles that should be implemented to ensure that it would be fair, transparent and credible.² The principles calling for a balanced representation in the proceedings, resources to enable civil society participation, and decision-making through consensus rather than by majority vote were ignored. As a result, the multistakeholder process is dominated by businesses and trade associations.

The first proceeding, to develop a code of conduct regarding mobile app transparency, was extremely divisive. Since no consensus was emerging among the participants, a subset of them, including some consumer and privacy organizations, decided to work on the side and drafted a code of conduct centered on a model privacy notice.³ This document was then presented to the larger group for a vote. Before the vote, serious questions about the efficacy of the privacy notice were raised by academics

¹ Federal Register Notice at www.ntia.doc.gov/files/ntia/publications/fr_privacy_rfc_notice_03052012_0.pdf.

² Comments of the World Privacy Forum et al, April 2, 2012, www.ntia.doc.gov/files/ntia/wpfetal_commerce_msprinciplesapril22012fs.pdf.

³ Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices, July 25, 2013, www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency.

who tested it on a random sample of 791 individuals as well as on four anonymous multistakeholder participants.⁴ They found that there was a low level of agreement about how different data and entities fit into the categories used in the notice, even among those who were directly involved in the multistakeholder process. This information was largely ignored. The vote was *not* on whether to approve the code but on whether to continue with the work. The majority voted not to continue and so the code was released in 2013 as a consensus document, though it was strongly criticized by some of the participants.⁵

Three years later, it is still not clear who has actually adopted the code and how it is working.⁶ We know of no published tests or studies that show how many consumers have actually read the notice, whether consumers understand it, and whether it accurately reflects the privacy practices of the apps that are using it. There does not appear to be any evidence that it is a success.

The second NTIA multistakeholder process, to develop a code of conduct for the use of facial recognition technology, was even more contentious than the first. Initiated in December 2013, it was finally concluded on June 15, 2016, but without the participation of any consumer and privacy groups. Some left the process early on; the remaining consumer and privacy groups walked out in June 2015 when it became clear that no consensus could be reached on even the most fundamental issues such as whether consumers should be asked for consent before their facial images are collected and used for purposes of facial recognition.⁷ The “best practice recommendations” (participants having rightly concluded that “code of conduct” is not an accurate term to use) that have been adopted⁸ are so weak that they cannot be taken seriously. They provide scant guidance for businesses and no real privacy protection for individuals.⁹

The third multistakeholder effort, which began in March 2015 and ended in May 2016, did successfully reach consensus among industry and consumer and privacy groups on best practices concerning privacy,

⁴ Rebecca Balebako, Richard Shay and Lorrie Faith Cranor, *Is Your Inseam a Biometric? Evaluating the Understandability of Mobile Privacy Notice Categories*, Carnegie Mellon University, July 17, 2013, https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab13011.pdf.

⁵ For instance, Consumer Federation of America stated that the model notice was not only confusing but misleading, see http://consumerfed.org/press_release/cfa-on-the-ntia-short-form-notice-code-of-conduct-to-promote-transparency-in-mobile-applications/. See also statements of Consumer Watchdog, www.consumerwatchdog.org/newsrelease/effort-craft-apps-%E2%80%9Ctransparency-code%E2%80%9D-shows-futility-multi-stakeholder-process, and Center for Digital Democracy, <https://www.democraticmedia.org/cdd-urges-ftc-review-proposed-ntia-code-conduct>.

⁶ See Natasha Singer, “Why a Push for Online Privacy is Bogged Down in Washington,” *New York Times*, February 28, 2016, noting that while Intuit introduced the notices in its QuickBooks Online Mobile Apps, many other companies have not adopted them, www.nytimes.com/2016/02/29/technology/obamas-effort-on-consumer-privacy-falls-short-critics-say.html?_r=0. We do not know of any list maintained by the NTIA documenting adoption of the code.

⁷ See group statement at http://consumerfed.org/pdfs/6-16-15%20Privacy%20Advocates%20Statement%20on%20NTIA%20Facial%20Recognition%20Process_Comments.pdf.

⁸ Information at www.ntia.doc.gov/other-publication/2016/privacy-multistakeholder-process-facial-recognition-technology.

⁹ See statement of consumer and privacy groups at http://consumerfed.org/press_release/statement-ntia-privacy-best-practice-recommendations-commercial-facial-recognition-use/.

transparency and accountability in the use of unmanned aircraft systems.¹⁰ This is perhaps a less contentious subject, implicating less well-entrenched business models, and most of the industry groups that participated were not the same as those who were involved in the first two proceedings. It remains to be seen how many entities adopt these best practices.

To our knowledge, the NTIA does not monitor adherence to the best practices or codes of conduct that come out of its multistakeholder proceedings, analyze their effectiveness, handle complaints related to them, or enforce compliance. Because of these limitations, the NTIA multistakeholder process does not have the elements of a good self-regulatory program.¹¹ The Federal Trade Commission can take legal action against companies that publicly commit to follow the NTIA codes of conduct or best practices and fail to do so, but we are unaware of any investigations or enforcement actions in connection with them so far.

The NTIA multistakeholder process will not work to protect broadband customers' privacy

There is no basis on which to argue that consensus on effective broadband privacy protection could be achieved through the NTIA multistakeholder process, or any similar process. As a recent report by the Center for Digital Democracy reveals, Internet service providers and other leading video providers are already deploying “powerful layers of data collection and digital marketing technologies to better target individuals.”¹² In the absence of a comprehensive privacy law in the United States, a vast system has grown to collect, analyze, and monetize data about individuals, across platforms and devices. The suggestion that Internet service providers will voluntarily agree to limit this data collection and use or give consumers real control is not borne out by our experiences. Furthermore, given the limitations of the NTIA multistakeholder process as described above, the outcome of such a process would not be mandatory for Internet service providers to follow or provide consumers with enforceable rights.

We note that industry blocked progress in another multistakeholder proceeding to protect online consumers' privacy, the World Wide Web Consortium's (W3C) efforts to develop standards for honoring do-not-track signals from consumers' Internet browsers. The modest aim of the proceeding was to make it easy for consumers to avoid online behavioral tracking. After the Digital Advertising Alliance (DAA) dropped out of the process in 2013, it has been moribund.¹³

Self-regulation alone cannot provide adequate privacy protection

The DAA's self-regulatory program to enable individuals to opt-out of behavioral advertising has been criticized for being confusing for individuals to navigate¹⁴ and garnering very low levels of public

¹⁰ Information at www.ntia.doc.gov/other-publication/2016/multistakeholder-process-unmanned-aircraft-systems.

¹¹ See *Self-Regulation: Role and Use in Supporting Consumer Interests*, Committee on Consumer Protection, Organization for Economic Cooperation and Development, March 2015, which describes the elements for effective self-regulation,

[www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CP\(2014\)4/FINAL&docLanguage=En](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CP(2014)4/FINAL&docLanguage=En).

¹² www.democraticmedia.org/sites/default/files/field/public-files/2016/ispbigdatamarch2016.pdf.

¹³ See Lou Mastria, “Digital Advertising Alliance Exits Do Not Track Group,” Adweek, September 17, 2013, www.adweek.com/news/technology/digital-advertising-alliance-exits-do-not-track-group-152475.

¹⁴ See Pedro G. Leon, Blase Ur, Rebecca Balebako, Lorrie Faith Cranor, Richard Shay, and Yang Wang, *Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising*, October 31, 2011 (revised May 10, 2012), Carnegie Mellon University, www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11017.pdf.

awareness and participation.¹⁵ Questions have also been raised about compliance with this and similar self-regulatory programs.¹⁶

The World Privacy Forum has documented the failure of many efforts to protect individuals' privacy through self-regulation.¹⁷ This includes industry programs and government initiatives such as the Safe Harbor program to enable U.S. companies to transfer Europeans' personal data to the United States, which was invalidated by Europe's highest court as inadequate to protect citizens' privacy.¹⁸

In a 2000 report to Congress, the Federal Trade Commission (FTC) noted that while it had previously expressed hope that self-regulation would achieve adequate online protection for consumers and urged Congress to refrain from enacting legislation, "Because self-regulatory initiatives to date fall far short of broad-based implementation of self-regulatory programs, the Commission has concluded that such efforts alone cannot ensure that the online marketplace as a whole will follow the standards adopted by industry leaders."¹⁹ The FTC recommended that Congress enact legislation that would set basic standards of practice and "provide an implementing agency with the authority to promulgate more detailed standards..."²⁰ Over time, the FTC became even more impatient with self-regulation, stating in a 2010 draft report that "industry efforts to address privacy through self-regulation have been too slow, and up to now have failed to provide adequate and meaningful protection."²¹ By 2012 when the FTC finalized that report, it called for Congress to consider enacting baseline privacy legislation.²² The Administration also called for privacy legislation in a 2012 report, "Consumer Data Privacy in a Networked World,"²³ while also suggesting that a multistakeholder process could be helpful as part of a comprehensive approach to addressing privacy issues.

¹⁵ See Kate Kay, "Study: Consumers Don't Know What AdChoices Privacy Icon Is," *AdvertisingAge*, January 2014, <http://adage.com/article/privacy-and-regulation/study-consumers-adchoices-privacy-icon/291374/>, Wendy Davis, "Most People Don't Understand 'AdChoices' Icon, The Daily Online Examiner Policy Blog, May 26, 2015, www.mediapost.com/publications/article/250688/most-people-dont-understand-adchoices-icon.html.

¹⁶ See Saranga Komanduri, Richard Shay, Greg Norcie, Blase Ur, Lorrie Faith Cranor, *AdChoices? Compliance with Online Behavioral Advertising Notice and Choice Requirements*, Carnegie Mellon University, March 30, 2011 (revised October 7, 2011), www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11005.pdf.

¹⁷ Robert Gellman and Pam Dixon, *Many Failures: A Brief History of Privacy Regulation in the United States*, World Privacy Forum, October 14, 2011, www.worldprivacyforum.org/wp-content/uploads/2011/10/WPFselfregulationhistory.pdf.

¹⁸ See Natalia Drozdiak and Sam Schechner, "EU Court Says Data-Transfer Pact With U.S. Violates Privacy," *Wall Street Journal*, October 6, 2015, <http://www.wsj.com/articles/eu-court-strikes-down-trans-atlantic-safe-harbor-data-transfer-pact-1444121361>.

¹⁹ *Privacy Online: Fair Information Practices in the Electronic Marketplace*, Federal Trade Commission, May 2000, <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf>, at 35.

²⁰ *Id.* at 36.

²¹ *Protecting Consumer Privacy in an Era of Rapid Change*, Federal Trade Commission Preliminary Staff Report, December 2010, at iii, <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf>.

²² *Protecting Consumer Privacy in an Era of Rapid Change*, Federal Trade Commission, March 2012, <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> at 12.

²³ See www.whitehouse.gov/sites/default/files/privacy-final.pdf, at 35.

To be clear, we are not opposed to voluntary codes of conduct, best practices, or other means of providing guidance to encourage good business practices. Some consumer and privacy groups have even initiated such efforts. For example, Consumer Federation of America (CFA) produced Best Practices for Identity Theft Services, which include privacy-related provisions, with input from consumer organizations and industry,²⁴ and the Center for Democracy & Technology (CDT) recently worked with Fitbit to develop guidelines for privacy and research for the health wearable industry.²⁵ Because CFA and CDT led these initiatives, they were able to ensure that consumer welfare was the core objective. We see these types of efforts as complementing legislation and rulemaking, not substituting for them.

The FCC should not defer to a multistakeholder process or self-regulation to protect broadband customers

Some commenters have encouraged the FCC to defer to multistakeholder forums or self-regulation to protect broadband customers' privacy. For example, AT&T said in its comments that "the Commission should rely on privacy guidelines developed by industry bodies and multistakeholder processes,"²⁶ Comcast suggested that "the FCC could defer this proceeding and use a multistakeholder process that the FCC convenes, working closely with both the FTC and NTIA to identify issues and solutions in the context of the principles that have been an important part of the Internet's success thus far,"²⁷ and Verizon said that "Given the complexity of issues affecting Internet privacy and security, the wide range of interested stakeholders, and the long history of effective self-regulatory initiatives in the context of privacy, a multi-stakeholder approach would be a more effective alternative to traditional, prescriptive regulation."²⁸

We are not surprised that businesses that would be affected by the FCC's proposed rules for broadband privacy would rather that it defer to a multistakeholder process or self-regulation to address privacy protection, because the resulting codes of conduct or best practices would be voluntary and unlikely to ask them to make any significant changes to their practices – changes such as asking consumers for their affirmative consent to use or share their data for secondary purposes.

It is surprising, however, that some of the groups that represent minorities are advocating for the FCC to turn to the NTIA's multistakeholder process. For example, the comments from the Multicultural Media, Telecom and Internet Council, Blacks in Government, Consumer Policy Solutions, Hispanic Technology and Telecommunications Partnership, LGBT Technology Partnership, National Black Caucus of State Legislators, National Coalition of Black Civic Participation, National Organization of Black County Officials, and National Puerto Rican Chamber of Commerce state that "To the extent that the

²⁴ <http://consumerfed.org/pdfs/CFA-Best-Practices-Id-Theft-Services.pdf>.

²⁵ See press release at <https://cdt.org/press/cdt-and-fitbit-develop-guidelines-for-privacy-and-research-for-wearables-industry/>.

²⁶ AT&T, <http://apps.fcc.gov/ecfs/document/view?id=60002080023> at 1.

²⁷ Comcast, <http://apps.fcc.gov/ecfs/document/view?id=60002081094> at 21.

²⁸ Verizon, <http://apps.fcc.gov/ecfs/document/view?id=60002078934> at 16. See also comments by CTIA, <http://apps.fcc.gov/ecfs/document/view?id=60002064853> at 4 and comment by the Internet Commerce Coalition that "the Department of Commerce has advocated use of multistakeholder negotiations to privacy issues raised by specific technologies, in lieu of unilateral statements by regulators," <http://apps.fcc.gov/ecfs/document/view?id=60002081118> at 7.

Commission believes more efforts are needed to protect consumer privacy, the agency should begin by engaging with the NTIA to convene a multistakeholder process to focus on the particular issues associated with consumer uses of broadband networks...²⁹

To our knowledge, none of these groups have participated in any of the NTIA proceedings. Since there is no evidence that the codes or best practices that emerge from them are effective, it is not clear on what basis these groups support them. Plus, given the voluntary nature of the process and its outcomes, it would not “ensure that all companies are subject to the same rules of the road.”³⁰ Codes of conduct and best practices are not rules that must be followed. Moreover, given our experience with the NTIA multistakeholder process, we believe that it is unlikely that such codes or best practices would be strong enough to adequately address the important concerns that civil rights groups have raised about big data and the potential for profiling and stereotyping.³¹

Conclusion

Despite numerous white papers and reports that have been produced over the last several years, conferences and workshops that have been held, and self-regulatory initiatives that have been launched, there has been no real progress on effectively protecting individuals’ privacy (except for strengthening the rules under the Children’s Online Privacy Protection Act, under which the Federal Trade Commission can promulgate privacy rules). This rulemaking is an opportunity to make progress in a crucial area, the privacy of our broadband communications.

The FCC should not be swayed by self-serving or ill-informed arguments that its proposed rules are not needed because market players will police themselves. It must exercise its authority to protect the privacy of broadband customers’ personal information. Consumer, privacy, and civil rights groups should work together to support the FCC’s proposed rules and push for strong, comprehensive privacy legislation.

Submitted by:

Center for Digital Democracy

Consumer Action

Consumer Federation of America

Consumer Watchdog

Privacy Rights Clearinghouse

²⁹ <http://apps.fcc.gov/ecfs/document/view?id=60002081105> at 8.

³⁰ *Id* at 9.

³¹ See *Civil Rights Principles for Big Data*, 2014, www.civilrights.org/press/2014/civil-rights-principles-big-data.html.