Data&Society RESEARCH INSTITUTE

Data & Society Research Institute Comments to NTIA on "Stakeholder Engagement on Cybersecurity in the Digital Ecosystem"

Docket No. 150312253-5253-01

May 27, 2015

I. Summary

The expanding digital economy and the Internet of Things (IoT) are changing every aspect of Americans' lives. With promises of personalization and efficiency that, to the credit of the companies offering these products, are often realized, Americans are persuaded to bring connected devices into their homes, wear connected devices on their bodies, and trust opaque algorithms to deliver news, search results, social networking services, and shopping services.

These services are new, imperfect and raise questions and dilemmas that have yet to be solved, and often are only starting to be addressed. The National Telecommunication and Information Administration should, as part of its multistakeholder process on security, privacy, and civil liberties in the digital ecosystem, aim to address the following questions:

1) How can companies ensure that their services, especially IoT devices, employ strong encryption and are protected by secure passwords? How can this be achieved given these devices' small screens and short battery life?
2) How can users be given substantive notification of what data is being collected about them, and how can companies implement procedures allowing them to meaningfully respect user choice of what to share?
3) How can multistakeholder participants ensure that user privacy and civil liberties are respected by all parties with access to data or devices?
4) What procedures should be put in place to ensure that service providers, in attempting to improve their services, learn about their customers, or achieve social goals, follow relevant ethical guidelines and respect the privacy and expectations of their users?

II. Introduction

The Data & Society Research Institute (D&S) welcomes the opportunity to submit this comment in response to the National Telecommunication and Information Administration's (NTIA) Request for Comments (RFC) dated March 19, 2015. The RFC asked members of the commercial, academic, and civil societies for feedback on which substantive cybersecurity issues affect the digital ecosystem and where broad, consensual action can improve user experience and safety.

D&S strongly supports efforts by the NTIA and industry actors to protect the security, privacy, and civil liberties of users in the digital ecosystem. The rapid expansion of connected devices into our homes, onto our bodies, and throughout our commercial, industrial, and recreational environments is far outpacing established law and social norms. For all their usefulness, these devices and the systems they run on may pose serious, if unintentional, risks to users. For example: users could find themselves sharing data with private companies whom they never intended to give access; user data could be misused, intentionally or unintentionally, denying users access to opportunities based on improperly considered characteristics; or user data could be leaked or stolen.

Given the number of devices, systems, and companies operating in the digital ecosystem, all the risks above are sure to happen; no security system is perfect, and the proliferation of connectivity will only increase the complexity of the systems and the number of incidents, eroding user trust in the system. The NTIA, along with privacy advocates, companies, researchers, and technologists, is well positioned to deal with these issues before users have their experience spoiled and companies lose the trust of their customers.

Given the expanding but relatively unexplored nature of the digital economy and the IoT, NTIA's call for a multistakeholder process is a timely and consequential step in ensuring the safeguarding of privacy and civil liberties. Based on our Institute's experience researching related issues and our diverse academic and applied backgrounds, we believe the multistakeholder process should focus on the proliferation of small, connected devices and the IoT. Within this realm, issues of cybersecurity, privacy, and civil liberties must be addressed. Specifically the multistakeholder process should address the following core issues:

- What is the scope of the privacy and civil liberties concerns raised by the digital ecosystem;
- What data is collected, and how is it used;
- What is the process by which users are informed about the collection and use of their data; and
- What are the possible civil liberties and privacy violations enabled by collecting vast amounts of data by devices that monitor intimate parts of users' lives?

III. Data & Society Research Institute

Data & Society is a research institute in New York City that is focused on social, cultural, and ethical issues arising from data-centric technological development.[1] The issues that D&S seeks to address are complex. The same innovative technologies and sociotechnical practices that enable novel modes of interaction, new opportunities for knowledge, and disruptive business paradigms can also be abused to invade people's privacy, provide new tools for discrimination, and harm individuals and communities.

To provide frameworks that can help society address emergent tensions, D&S is committed to identifying issues at the intersection of technology and society, providing research that can ground public debates, and building a network of researchers and practitioners that can offer insight and direction.

[1] Data & Society Research Institute, http://www.datasociety.net/.

To advance public understanding of the issues, D&S brings together diverse constituencies, hosts events, does directed research, creates policy frameworks, and builds demonstration projects that grapple with the challenges and opportunities of a data-soaked world. D&S weaves together researchers, entrepreneurs, activists, policy creators, journalists, geeks, and public intellectuals to debate and engage one another on the key issues.

Current institutional research initiatives include: Data & Fairness; the Future of Labor in a Data-Centric Society; Enabling Connected Learning; Intelligence and Autonomy; Ethics in "Big Data" Research; and Privacy. These initiatives are joined by projects in different states of maturity covering financialization, crowd labor, workplace surveillance, science fiction, the market for privacy, data and human rights, urban science, evidence in health policymaking, infrastructure, and magic.

IV. Expanding Digital Economy

Computers are being integrated into nearly every aspect of Americans' lives. Not only do computer-run algorithms mediate our shopping and social experiences,[2] but increasingly small and ubiquitous devices track our movements and monitor our bodies and environments in our offices, social spaces, and even in our homes. These devices often collect intimate information about our lives. Fitness trackers monitor our location, our activity level, and our heartbeats, recording information for use by insurance companies;[3] smart thermostats and smoke alarms monitor our comings and goings from our houses and particular rooms within them; connected security systems keep a digital eye on our most intimate spaces; cell phones, desktop and laptop computers, and video game consoles are more and more often always on and always listening for our next voice command.[4] These devices are often controlled by complicated and opaque algorithms[5] and outfitted with increasingly smaller screens—if any—that could be used to accept user input or inform users about privacy or security implications of their use. They are not only being embraced by some of the largest technology companies in America, but are being wholeheartedly embraced by internet users, who may implicitly trust the devices they purchase and services they use. However, significant privacy and civil liberties concerns remain unaddressed by the industry.

[2] *See, e.g.*, Amit Chowdhry, *Facebook Changes News Feed Algorithm To Prioritize Content From Friends Over Pages*, Forbes (April 23, 2015), http://www.forbes.com/sites/amitchowdhry/2015/04/23/facebook-changes-news-feed-algorithm-to-prioritize-content-from-friends-over-pages/; Jessica Leber, *Amazon Woos Advertisers with What It Knows about Consumers*, MIT Technology Review (Jan. 21, 2013), http://www.technologyreview.com/news/509471/amazon-woos-advertisers-with-what-it-knows-about-consumers/.

[3] Lucas Mearian, *Insurance company now offers discounts – if you let it track your Fitbit*, Computer World (Apr. 17, 2015), http://www.computerworld.com/article/2911594/insurance-company-now-offers-discounts-if-you-let-it-track-your-fitbit.html.

[4] *See, e.g.*, T.C. Sottek, *The Xbox One will always be listening to you, in your own home (update)*, The Verge (May 21, 2013), https://www.theverge.com/2013/5/21/4352596/the-xbox-one-is-always-listening; David Lee, *Moto X 'always listening' phone launched by Google's Motorola*, BBC News (Aug. 1. 2013), http://www.bbc.com/news/technology-23536936.

[5] Mathew Ingram, *Giants behaving badly: Google, Facebook and Amazon show us the downside of monopolies and black-box algorithms*, GigaOm (May 23, 2014), https://gigaom.com/2014/05/23/giants-behaving-badly-google-facebook-and-amazon-show-us-the-downside-of-monopolies-and-black-box-algorithms/.

Many of the services and devices that Americans use every day are opaque in their collection and use of data; not only is this collection and use passive and invisible to users, but it is often too complex for users to fully understand how the services operate. Further, many companies keep the inner workings of their services secret. Personalized online services offering shopping, access to social networks, or displaying ads are central to many users' online experiences, and collect data about all of their online activity, either for internal use or for sale to other companies. However, users are often unaware of what data is being collected or precisely how it is used. Perhaps more problematically, users are rarely able to opt-out of such collection or use, and even when they are, the procedure is often dauntingly complex.[6] As these services and devices continue to proliferate and to grow more complex, security breaches and privacy invasions will surely become more common. User trust—and buy-in for new devices—will become commensurately harder to maintain. By addressing privacy and civil liberties concerns now, the companies offering these services and devices have the chance to increase user safety and privacy and gain user trust in the process.

V. Privacy Questions

The multistakeholder process should seek to address a number of privacy concerns raised by online services and IoT devices. First, the multistakeholder process should identify the scope of the cybersecurity problem faced by the industry. Many IoT devices are small and low-powered, making encryption of transmitted data difficult. Further, they often have small screens, if they have them at all, and can be part of complex home networks, raising the possibility that new software updates will go unnoticed or uninstalled for fear of disrupting the wider system. Participants in the multistakeholder discussion should determine to what degree these problems are leading to security breaches or privacy invasions in the real world. By determining the scope of the problem, participants can better tailor the efforts to protect user privacy and maintain user trust.

Second, participants should discuss how to address weak or nonexistent encryption protocols and poor security practices. Strong encryption is necessary to protect the security and privacy of internet users.[7] However, many services use weak encryption protocols—or none at all—even while providing users a semblance of security.[8] IoT devices need particular attention. Due to their small size, low power

[6] *See Facebook Privacy: A Bewildering Tangle of Options*, New York Times (May 12, 2010), http://www.nytimes.com/interactive/2010/05/12/business/facebook-privacy.html?_r=0 ("To manage your privacy on Facebook, you will need to navigate through 50 settings with more than 170 options."); Vindu Goel, *Flipping the Switches on Facebook's Privacy Controls*, New York Times (Jan. 29, 2014), http://www.nytimes.com/2014/01/30/technology/personaltech/on-facebook-deciding-who-knows-youre-a-dog.html ("In practice, though, adjusting Facebook's dozens of privacy controls can be tedious and confusing.").

[7] "There's no scenario in which we don't want really strong encryption." Kara Swisher, *Obama: 'There's No Scenario in Which We Don't Want Really Strong Encryption'*, Re/Code, https://recode.net/2015/02/13/obama-theres-no-scenario-in-which-we-dont-want-really-strong-encryption/ (last visited May 26, 2015) (quoting President Barack Obama).

[8] For example, Snapchat users have found that, contrary to the company's claims, their photos do not "disappear forever" after being seen. Katey Psencik, *Why students should be more careful with 'confidential' apps*, USA Today (July 10, 2013), http://www.usatoday.com/story/tech/personal/2013/07/10/students-security-snapchat-whisper/2506539/ (discussing SnapChat, Whisper, iOS, and Android).

draw, and difficulty updating their software while maintaining their function with other devices, implementing strong encryption on them could be difficult. Passwords are also problematic; many people use weak passwords, or fail to change the default password on their device. Additionally, passwords can be difficult to enter into small devices, or get in the way of the seamless operation of a system of IoT devices. Participants in the NTIA's multistakeholder process should come to an agreement on minimum encryption standards that their products and services will employ and find ways to encourage the use of strong passwords.

Third, the multistakeholder process should address ways to ensure that software updates are made available to users and installed regularly. Failure to update devices can leave users vulnerable to holes in security that have been long known and are easy to exploit. In the past, users have been slow to update or upgrade systems that are central to their computing experience.[9] Participants should aim to adopt standards that encourage releasing security updates often and methods for encouraging users to regularly download and install those updates.

Fourth, participants should address questions of data ownership raised by IoT installations in renter-occupied housing. It is generally assumed that the owner of IoT devices like thermostats, smoke detectors, light bulbs, and others will be the owner of the house in which they operate. But possible savings through efficiency will surely encourage developers and landlords to outfit their buildings with IoT devices, providing them with savings and their tenants with the convenience the devices bring. However, this could provide landlords with significant data about the private and intimate lives of their tenants, and could allow for landlords to exercise previously impossible levels of control and authority over those they are watching. Participants in the multistakeholder process should consider how they can ensure, through their terms of service or otherwise, that the end user who is actually operating the devices has access to the data collected; intermediaries who may have purchased or installed the devices, but who do not actually use or are not monitored by the devices should not be able to access user data.

Finally, the participants in the process should agree on standards for notifying users about what data is collected and how it is used,[10] and, most importantly, providing them actual choice in allowing the collection of that data that does not require they forgo using the product. The small size and background nature of IoT devices, and desire by service providers to provide streamlined and clean

[9] Ed Bott, *Why you should care about automatic updates for Flash Player*, ZDNet (March 29, 2012), http://www.zdnet.com/article/why-you-should-care-about-automatic-updates-for-flash-player/#! ("If you allow people to decide whether they want to install updates or not, a nontrivial number will just say no, because it's a hassle. They will ignore prompts and warnings. They will continue using outdated software for which one or more critical updates is available.").

[10] Regulating only use, and not collection, of data would be inappropriate as it is impractical to expect users to be able to protect previously collected data from future uses. Further, the NTIA has already stressed the importance of transparency in the collection and sharing of data. *See*, Nat'l Telecomm. & Info. Admin., *Privacy Multistakeholder Process: Mobile Application Transparency* (Nov. 12, 2013), http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency.

experiences can make informing users difficult. When services are designed to blend into the background of a user's experience at home, in the gym, or while socializing online, it may be tempting to keep disclosures about data collection or controls concerning data use out of the way. However, this sort of information and control is central to maintaining user privacy to the standard of each individual user and to maintaining trust. Participants should address how to best give users substantive information about the types of data that are being collected. Users should be able to make informed opinions about what products to use, how to use them, and what data to provide access to. Users should also be clear about what kind of action they need to take to protect themselves in case of a security breach.

Most importantly, users should be given actual choice when it comes to what data is collected by the companies offering services and whether to agree to changes in terms of service. Privacy is personal and contextual; what one person is willing to disclose in a given context is not necessarily what all people would be comfortable revealing about themselves. Users should not be denied access to the use of new devices because their privacy concerns outstrip the protections provided by the offered services. The companies offering online services and connected devices should agree on a framework in which they can offer individual users simple, easy to understand choices about what data will be collected about them. While some of the promises of the digital economy are personalization and efficiency, privacy must be similarly valued. A user who wishes certain facts about themselves to remain private should be able to make that choice and trade a measure of personalization or efficiency for privacy.

VI. Civil Liberty Questions Remain Un-Addressed

The opaque nature of the algorithms that control our online services also presents dilemmas for user trust and civil liberties. These algorithms can be used to take advantage of users in new ways. Some groups have used bots designed to mimic humans on social networking sites to shape the ideas or actions of people on those social networks—a type of high-tech and largely invisible astroturfing.[11] Facebook has even experimented on its users, making attempts to influence their emotions by selectively showing items in their news feeds.[12]

Beyond the potential consumer harms, these companies have the potential to cause serious social and civil harm by manipulating users outright or by slightly adjusting their algorithms to achieve a particular, or even unintended, outcome. For example, Facebook and Google have, in recent years, displayed "I voted" buttons on profiles of users who told Facebook they had completed their civic

[11] Andy Isaacson, *Are You Following a Bot?*, The Atlantic (May 2011), http://www.theatlantic.com/magazine/archive/2011/05/are-you-following-a-bot/308448/.

[12] *See The Facebook Experiment: What It Means For You*, Forbes (Aug. 4, 2014), http://www.forbes.com/sites/dailymuse/2014/08/04/the-facebook-experiment-what-it-means-for-you/; Adam Kramer, Jamie Guillory, & Jeffrey Hancock, *Experimental evidence of massive-scale emotional contagion through social networks*, 111 Proc. of the Nat'l Acad. of Sci. of the U.S., no. 24 (June 2, 2014), *available at* http://www.pnas.org/content/111/24/8788.full.

duty[13] or provided tools to help users find their polling place.[14] Such measures, while well intended, can have social consequences, and we will surely see the effect of these services on our lives outside of elections. The ramifications become even more unsettling in a scenario in which the platforms themselves intentionally exert this influence. Some researchers have raised the threat posed by "digital gerrymandering", the selective use of voting buttons to influence user turnout to the polls.[15]

These technologies can also cause individual harms. Algorithms designed to select job candidates could perpetuate the hidden or unintentional biases of their programmers.[16] Search algorithms could bias job searches even earlier, by selectively displaying job advertisements to people of certain races, ethnicities, or genders, or could provide search results that bias employers against prospective employees with certain characteristics. Algorithms could also lead companies to improperly discriminate in the provision of loans to potential creditors. While lenders are forbidden from basing their lending decisions on racially discriminatory factors, complex and well-meaning algorithms could lead to harmful outcomes.

Addressing the collective and individual risks posed by these technologies should be weighed against an interest in encouraging innovation and experimentation in the space. IoT and the digital economy it supports promises to provide enormous benefits to consumers and unlock massive returns for investors. Striking a balance that mitigates the risks while maximizing the benefits is a critical challenge as this technology continues to emerge and mature.

First, a multistakeholder process should develop a set of best practices around the transparency of an algorithm to users. Participants could determine under what contexts a user should be permitted to request information about an algorithm with which they interact. What information is sufficient to be provided by a platform or a technology provider? Further, given the opacity, complexity, and, perhaps, proprietary nature of these algorithms, can a fair, thorough, and transparent third-party auditing process be adopted by the participants of the multistakeholder process?

Second, a multistakeholder process should address the methods of redress and control available to users. When does an algorithm engage in impermissible discriminatory practices? Who is responsible for the harms created by such a system? What tools are given to users to control the behavior of the systems they interact with? If users are to trust that the systems they interact with are providing unbiased responses to their inputs, the participants will need to notify users when something goes wrong and ensure that problems are remedied quickly and clearly.

[13] Micah Sifry, *Facebook Wants You to Vote on Tuesday. Here's How it Messed With Your Feed in 2012*, Mother Jones (Oct. 31, 2014), http://www.motherjones.com/politics/2014/10/can-voting-facebook-button-improve-voter-turnout.

[14] *Google Will Show You Where to Vote*, TechCrunch (Sep. 22, 2008), http://techcrunch.com/2008/09/22/google-will-show-you-where-to-vote/.

[15] Jonathan Zittrain, *Facebook Could Decide an Election Without Anyone Ever Finding Out*, New Republic (June 1, 2014), http://www.newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering.

[16] Alex Rosenblat, Tamara Kneese, & danah boyd, *Networked Employment Discrimination*, Data & Society Research Institute (Oct. 8, 2014), http://www.datasociety.net/pubs/fow/EmploymentDiscrimination.pdf.

Finally, the multistakeholder process should address the question of proactively using these technologies to better the public interest. Should platforms be permitted to engage in practices that attempt to shape social practices like voting in an effort to promote better turnout? Should platforms take action to expose users to crosscutting points of view? The obligations or needed forbearance of companies in engaging in these actions is as yet undefined. While experimentation on users has already caused public outcry, many more attempts will be made to understand or influence users, often with the goal of increasing a social good. Participant should determine when such influence or testing is inappropriate and agree upon a transparent thorough procedure to be followed.

VII. Suitability for Multi Stakeholder Process

Questions of user privacy and civil liberties in the digital economy are ripe to be addressed by an NTIA led multistakeholder process. These technologies are new and changing every day. Legislating privacy rules has already proven to be a difficult process, and attempting to determine rules for such a fast changing environment would likely be difficult for Congress. However, the technical and subject matter experts at the NTIA and industry participants of the multistakeholder process are well positioned to determine the scope of the risk to users' privacy and civil liberties and to agree upon reasonable and strong safeguards that will not only protect users, but gain and keep their trust. The expertise provided by the participants in the multistakeholder process, along with the fast moving nature of the digital economy make a voluntary, industry led effort a good step towards protecting user privacy and civil liberties.

To date, no forum has brought together the community of privacy advocates, companies, researchers, and technologists to strike a balance between these competing interests. NTIA has a unique opportunity to convene this group and produce consensus on these issues. Further, this group should have the ability and incentives to reach such an agreement.

Industry actors interested in gaining and maintaining user trust should be eager to adopt strong rules protecting user privacy and civil liberties now, before any major security breaches, privacy invasions, or scandals deter the public from using online services or IoT devices. While many Americans currently value their privacy and security, they are also willing to adopt new tools that require access to personal information or that collect data about their lives. That may not always be the case. It is far better to adopt strong rules governing corporate transparency, user privacy and security, and civil rights now, before user trust is shaken. The multistakeholder process can strengthen user trust by helping to ensure that users are safe, and is far easier than attempting to regain user trust after users have seen their privacy invaded or civil liberties injured.

Further, agreeing on a framework early in the adoption of these new and pervasive devices opens the field for innovation. Without any guidance as to what practices are safe or reasonable, companies with new ideas and innovative approaches may be unwilling to try something new. Agreeing on industry standards and adopting such a framework should protect companies who wish to offer new products and new services while allaying public fears that widespread adoption of technology will lead to decreased privacy or will damage civil liberties.

Data & Society thanks you for the opportunity to provide feedback. If you have any questions, please contact Zachary Gold at zack@datasociety.net.

Respectfully submitted,

Data & Society Research Institute