BEFORE THE
DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS & INFORMATION ADMINISTRATION

In the Matter of
The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things

Docket No. 160331306-6306-01

Comments of the Staff of the Federal Trade Commission's
Bureau of Consumer Protection and
Office of Policy Planning

June 2, 2016

The FTC also has pursued numerous policy initiatives designed to enhance consumer privacy. For example, the FTC has hosted workshops and issued reports to improve privacy disclosures in the mobile ecosystem, increase transparency in the data broker industry, examine the implications of big data on low-income and underserved consumers, and highlight the privacy and security implications of facial recognition and the Internet of Things.[10]

Finally, the FTC engages in consumer and business education to increase the impact of its enforcement and policy development initiatives. The FTC uses a variety of tools – brochures, online resources, workshops, and social media – to distribute educational materials on a wide range of topics, including mobile apps, children's privacy, and data security. On the business education front, most recently, the Commission launched its "Start with Security" initiative and "Careful Connections" IoT guidance, both of which include some lessons for businesses considering security issues in the IoT space.[11] On the consumer education front, the FTC recently announced the rollout of its enhanced IdentityTheft.gov website,[12] a free, one-stop resource people can use to report and recover from identity theft. Now, identity theft victims can use the site tr [(u)-c.2(, t)-2h.0023hTue site tu( )Tj 0.002 Tc -0.002 Tpebs n226 toolsethTubs a cudtea

business (“B2B”) electronic marketplaces[16]

consumers. This comment summarizes many of the findings and recommendations from the IoT Workshop and IoT Report.

A. Benefits

B. Risks

vulnerable connected car can lead to engine failure or a loss of control; and an insecure IoT alarm system can open up a home to danger.[33]

2. Privacy Risks

Beyond security risks, IoT devices also raise concerns about consumer privacy. Some privacy risks involve the direct collection of sensitive personal information, such as precise geolocation, financial account numbers, or health information.[34] Others arise from the collection of personal information, habits, locations, and physical conditions over time, which may allow an entity that has not directly collected sensitive information to infer it.[35]

In one FTC analysis, staff found the presence of

States, the FTC is responsible for enforcing the Children's Online Privacy Protection Act[40] and continues to protect the personal information of children

percent of those sites collected personally identifiable information from users.[45] Consumers are often unaware of this cross-device tracking, and have limited ability to opt out.[46]

3. Risks to Disadvantaged Communities

The RFC also asks about the impact that Internet of Things might have on disadvantaged or rural communities.[47] As noted above, data generated by IoT devices can support advances in energy, health care, and car safety, among others, and have a beneficial impact on low-income and underserved populations. On the other hand, inaccurate or biased analysis of IoT data can lead to consumers being denied opportunities for education, employment or credit. Companies may seek more data, including IoT data, in order to improve their analysis,[48] but having more data does not necessarily eliminate the risks of inaccuracy or bias. For example, an employment research firm found commuting distance to be one of the strongest predictors of how long a customer service employee will keep a job. But they realized that commuting distance is often correlated with race, and declined to use this predictor out of concern that using it would reduce workplace diversity and potentially violate equal employment opportunity standards.[49]

Earlier this year, the FTC issued a report on the impact of big data on underserved consumers, which describes such risks in more detail.[50] One specific challenge is ensuring or compensating for an incomplete data set. For example, Hurricane Sandy generated more than twenty million tweets between October 27 and November 1, 2012. The greatest number of tweets came from Manhattan, creating the illusion that Manhattan was the hub of the disaster. Very few messages originated from more severely affected locations, such as Breezy Point, Coney Island, and Rockaway – areas with lower levels of smartphone ownership and Twitter usage. As

[45] Id. (Cross Device Tracking Presentation, at event materials tab, Slide 33).

[46] See Ctr. for Dem. & Tech., Comments for November 2015 Workshop on Cross-Device Tracking, at 8 (Oct. 16, 2015), available at https://cdt.org/files/2015/10/10.16.CDT-Cross-Device-Comments.pdf (indicating that user understanding and transparency around cross-device tracking is very low); Elec. Privacy Info. Ctr, Comments of The

extended power blackouts drained batteries and limited cellular access, even fewer tweets came from the worst hit areas. If organizations were to base decisions on where to deploy emergency services on this incomplete data, the people who needed services the most might not have received them.[51]

IV. PRIVACY AND SECURITY RECOMMENDATIONS

Industry and government stakeholders both have an important role to play in fostering innovation in the Internet of Things while at the same time minimizing privacy and security risks.[52] As NTIA's recent analysis of Census data shows, negative privacy and security experiences can have a direct impact on consumer trust, which could lead to consequences for IoT innovation.[53] This section discusses the respective roles of industry and government in fostering innovation by building consumer trust.

A. Best Practices for Businesses

1. Security

There is widespread consensus that companies developing IoT products and services should implement reasonable security.[54] In creating their security programs, the FTC staff has recommended that, among other things, companies in the IoT space: (1) build security into their devices at the outset; (2) train employees on good security practices; (3) ensure downstream privacy and data protections through vendor contracts and oversight; (4) apply defense-in-depth strategies that offer protections at multiple levels and interfaces; and (5) put in place reasonable access controls.[55] The FTC's Careful Connections and Start with Security publications offer more detailed guidance.[56]

expectation that their privacy and security will be protected throughout the life of the product.[57] If this is not the case, companies should truthfully convey to consumers the extent to which they intend to provide security updates to their devices. When feasible, disclosing the length of time companies plan to support and release software updates for a given product line will help consumers better understand the security features' expiration dates for their Internet-connected devices.[58]

Where an IoT company fails to implement reasonable security, it could be violating the FTC Act's prohibition against deceptive and unfair practices. For example, in its first IoT case, the FTC brought an action against a company, TRENDnet, which sold Internet-connected cameras for purposes ranging from home security to baby monitoring. While advertising their products as secure, the FTC alleged that the company failed to build security into the design of their products, train their employees, implement a process for actively monitoring security vulnerabilities, and perform security tests.[59] In a more recent case against router manufacturer ASUS, the FTC charged that the company failed to reasonably secure the routers it sold to consumers, resulting in vulnerabilities that allowed hackers to gain unauthorized access into thousands of consumers' networks. Among other things, according to the complaint, the company failed to perform security reviews, code review and testing, or vulnerability and penetration testing. The complaint further alleged that the company failed to implement readily available, low-cost protections against reasonably foreseeable vulnerabilities.[60] Under the proposed order, ASUS must establish a comprehensive security program and notify consumers about software updates or other steps they can take to protect themselves from security flaws.[61]

2. Data Minimization

Data minimization refers to the concept that companies should limit the data they collect and retain, and dispose of it once they no longer need it. Staff recommends that companies in the IoT space should consider reasonable data minimization practices.[62]

Data minimization can help guard against two privacy-related risks. First, larger data stores present a more attractive target for data thieves, both outside and inside a company – and increases the potential harm to consumers from su(imiz)-4(a)4(l)-1.15 Td ( )Tj EMC4(bl)vonsumers d 1

retains large amounts of data, there is an increased risk that the data will be used in a way that departs from consumers' reasonable expectations.[63]

To minimize these risks, companies should examine their data practices and business needs and develop policies and practices that impose reasonable limits on the collection and retention of consumer data. However, recognizing the need to balance future, beneficial uses of data with privacy protection, staff suggests several options for companies to consider. They can decide not to collect data at all; collect only the fields of data necessary to the product or service being offered; collect data that is less sensitive; or deidentify the data they collect.[64] If a company determines that none of these options will fulfill its business goals, it can seek consumers' consent for collecting additional, unexpected categories of data, as explained below.[65]

3. Notice and Choice

Consumer choice continues to play an important role in the IoT. Some stakeholders have suggested that offering notice and choice is challeng helfi i-2(su')3(c) ( )Tj6(l)-2f()2a 0 Td ub8f()-qu t 6

The establishment of legislative or widely accepted multistakeholder frameworks could potentially address some of these concerns by designating permitted or prohibited uses. In the absence of consensus on such frameworks, however, the approach set forth in giving consumers information and choices about their data – continues to be the most viable one for the IoT in the foreseeable future.[75]

4. Big Data

Given the risks associated with big data analytics of IoT products described above, in addition to complying with existing legal requirements,[76] companies should be aware of existing academic research on how certain uses of big data sets may lead to inaccurate or biased results.[77] This research suggests that companies should consider the following when engaging in big data analytics of IoT data:

- Consider whether their data sets are missing information from particular populations, and if they are, take appropriate steps to address this problem.
- Review their data sets and algorithms to ensure that hidden biases do not have an unintended or disparate impact on certain populations.
- Note that, just because big data found a correlation, that does not necessarily mean the correlation is meaningful. As such, companies should consider the risks of using those results, especially where their policies could negatively affect certain populations. It may be worthwhile to have human oversight of data and algorithms when big data tools are used to make important decisions, like ones implicating health, credit, and employment.
- Consider whether ethical considerations advise against or in favor of using big data in certain circumstances. Companies should consider whether they can use big data in ways that advance opportunities for previously underrepresented populations.[78]

B. The Role of Government in Fostering the IoT

Government can play an important role in protecting consumers while supporting innovation in the IoT. For its part, through speeches and other industry and consumer outreach, Congressional testimony, and advocacy comments such as this one, the FTC will continue to promote the best practices described in this comment and its IoT Report. The FTC will also continue to take enforcement action against IoT companies that violate the laws enforced by the FTC.

Staff believes that IoT-specific privacy and data security legislation would be premature at this time. However, the FTC's efforts could be enhanced by appropriate legislation. For this

[75] Id.
[76] The FTC's Big Data Report highlights laws that might apply to big data, including the FTC Act, Fair Credit Report Act, and equal opportunity laws. See Big Data Report at iv.
[77] See generally Big Data Report at vi and 1-5. As one example of research on this issue, see Kate Crawford, The Hidden Biases in Big Data, Harv. Bus. Rev. (2013), https://hbr.org/2013/04/the-hidden-biases-in-big-data
[78] Big Data Report at iv. See also Lesley Fair, Why Big Data is a Big Deal, Fed. Trade Comm'n (Jan. 6, 2016) (blog), available at https://www.ftc.gov/news-events/blogs/business-blog/2016/01/why-big-data-big-deal

reason, the FTC has recommended that Congress enact general (as opposed to IoT-specific) security and privacy legislation. First, the FTC continues to support flexible, technology-

allowing products to interoperate in a predictable manner.[83] These standards may increase competition by eliminating switching costs for consumers who want to utilize products

different and competing technical approaches to interoperability may provide stronger privacy and data security benefits to consumers compared to a marketplace with a single interoperability standard. Further, a marketplace with competing technical approaches would induce firms to innovate to develop interoperability solutions with privacy and data security attributes desired by consumers. When considering standardization and the interoperability of technologies, NTIA should carefully balance the potential benefits and costs to consumers and firms of standardization and competition.

VI. CONCLUSION

Staff hopes that this information, as expanded in greater detail in its 2015 Internet of Things Report, has been of assistance in furthering NTIA's survey of the IoT environment and the impact of IoT devices on the privacy and security of consumers and their w1-2(j -0.00)nnd