BEFORE THE UNITED STATES FEDERAL TRADE COMMISSION

WASHINGTON, DC

COMMENTS OF THE FUTURE OF PRIVACY FORUM	)
RE: INTERNET OF THINGS, PROJECT NO. P135405	)

I. Introduction

On November 19, 2013, the FTC held a Workshop examining the privacy and security issues associated with connected "smart technologies," collectively referred to as the "Internet of Things."[1] The Future of Privacy Forum ("FPF")[2] was pleased to participate in the Workshop's panel on Connected Cars. Following the event, the FTC invited public comments to further the Commission's understanding of the issues raised at the Workshop.[3] FPF appreciates this opportunity to provide these Comments on those issues and to submit formally FPF's white paper, *An Updated Privacy Paradigm for the "Internet of Things"*, which FPF published to coincide with the Workshop, attached as Appendix A to these Comments.

The Internet of Things has been an important focus of FPF's work since our founding in 2008. FPF recognizes the enormous potential benefits to consumers and to society of the inter-connected applications offered through the Internet of Things.[4] At the same time and from the beginning, FPF has worked to ensure that privacy and security are integrated into those implementations of the Internet of Things that involve the collection and sharing of personal

1 *Internet of Things—Privacy and Security in a Connected World*, FTC, *available at* http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-and-security-connected-world (last visited Jan. 10, 2014).

2 The Future of Privacy Forum is a Washington, D.C.-based think tank whose mission is to advance privacy for people in practical ways that allow for innovation and responsible use of data. The FPF Advisory Board includes privacy professionals, privacy scholars, and academics. The co-chairs of FPF are Jules Polonetsky, its Executive Director, and Christopher Wolf, who leads the global privacy practice at Hogan Lovells US LLP.

3 *FTC Seeks Comment on Issues Raised at Internet of Things Workshop Project No. P135405*, FTCPublic.commentworks.com, https://ftcpublic.commentworks.com/ftc/netofthingsworkshop/ (last visited Jan. 10, 2014).

4 The array of consumer benefits coming from the Internet of Things was underscored by the focus on connected devices at the recent 2014 Consumer Electronics Show. *See, e.g.*, Kim Peterson, *"Internet of Things" All the Rage at Consumer Electronics Show*, CBSNews.com (Jan. 7, 2014 8:49 a.m.), http://www.cbsnews.com/news/internet-of-things-all-the-rage-at-consumer-electronics-show/.

information. Starting with our original and ongoing project on the smart grid, an early white paper on Privacy by Design in the smart grid (jointly authored with Information and Privacy Commissioner of Ontario, Ann Cavoukian, Ph.D.),[5] and continuing to include our current work on "connected cars" and "smart stores,"[6] FPF has acquired experience and insights into the technologies and services associated with connected device ecosystems. With respect to data privacy, we have learned that traditional privacy principles can provide useful guidance when developing data practices for the Internet of Things and that new technologies sometimes require new implementation approaches or different applications of those underlying principles. FPF is pleased to share its insights into how to promote privacy and security without sacrificing the substantial consumer benefits that the Internet of Things has to offer.

In these Comments, we begin by expanding on the discussion from our White Paper on the appropriate privacy paradigm for the Internet of Things. We then address what we believe to be two of the important themes raised during the Workshop: 1) the importance of data security and 2) the privacy issues raised by the comprehensive collection of information. And we conclude with some further thoughts on how consumer privacy can be promoted in the Internet of Things.

II. FPF White Paper: *An Updated Privacy Paradigm for the "Internet of Things"*

Coinciding with the FTC's Internet of Things Workshop, FPF published a White Paper[7] discussing the appropriate framework for the privacy issues raised by the Internet of Things. As we indicated in our White Paper, and as presented at the Workshop, the Internet of Things promises to deliver a range of economic and social benefits.[8] As the Internet of Things matures,

---

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

6 FPF is providing leadership on the use of mobile location analytics in the retail environment and the associated privacy issues. *See Smart Stores*, Future of Privacy Forum, http://www.futureofprivacy.org/issues/smart-stores/.

7 Christopher Wolf & Jules Polonetsky, *An Updated Privacy Paradigm for the "Internet of Things"* (2013) [hereinafter FPF White Paper] (attached as Appendix A).

8 Future of Privacy Forum, Comments of the Future of Privacy Forum on Connected Smart Technologies in Advance of the FTC "Internet of Things" Workshop (May 31, 2013) [hereinafter Prior FPF Comments], *available at* http://www.ftc.gov/sites/default/files/documents/public_comments/2013/07/00013-86159.pdf. Chairwoman Ramirez noted in her opening remarks for the Workshop that the consumer benefits of the Internet of Things "will no doubt be great." Opening Remarks of FTC Chairwoman Edith Ramirez, The Internet of Things: Privacy and Security in a Connected World (Nov. 19, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/opening-remarks-ftc-chairwoman-edith-ramirez-federal-trade-commission-internet-things-privacy/131119iotremarks.pdf. Commissioner Ohlhausen has stated that "[t]he Internet of Things has the potential to

we will likely witness significant improvements and surprising innovations in the areas of health care, transportation, communications, education, personal and public safety, resource management, and more. The framework discussed in our White Paper is designed to promote privacy in the Internet of Things without sacrificing those important benefits.

The Fair Information Practice Principles ("FIPPs") are a valuable set of high-level guidelines for promoting privacy. As we noted in our comments submitted in advance of the Workshop, "[FIPPs] still are germane even if their adaptability is unique,"[9] and there is no need to abandon the FIPPs. However, they can be implemented and adapted to the Internet of Things or other contexts in a variety of ways. As the FTC itself has recognized, stakeholders are well-positioned to design and develop mechanisms and standards that are tailored for particular business models and contexts—and informed by traditional principles.[10] The White House has also recognized that privacy protections should be developed in a manner that reflects "the FIPPs in a way that emphasizes the importance of context in their application."[11]

In its White Paper, FPF notes that, given the nature of the technologies involved, *traditional* implementations of the FIPPs may not always be practical as the Internet of Things matures. This should come as no surprise. The FIPPs are not meant to establish a rigid set of guidelines for the processing of information. Instead, they are designed to serve as high-level guidelines.[12] While the traditional mechanisms—such as presentations of detailed privacy policies and prompts for consents—have served to promote the FIPPs in many contexts, new mechanisms may be appropriate for some implementations of the Internet of Things.[13]

Rather than insisting on traditional implementations of the FIPPs universally across the Internet of Things, we encourage the FTC to support the ongoing efforts of industry and other stakeholders to develop flexible, use-based standards that are tailored to the contexts of

---

transform many fields." Remarks of Commissioner Maureen K. Ohlhausen, The Internet of Things: When Things Talk Among Themselves, FTC Internet of Things Workshop (Nov. 19, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/remarks-commissioner-maureen-k.ohlhausen-ftc-internet-things-workshop/131119iotspeech.pdf.

9 Prior FPF Comments, *supra* note 8, at 2.

10 *See* FTC, Protecting Consumer Privacy in an Era of Rapid Change 49-50 (2012).

11 The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy 16 n.21 (2012).

12 *See, e.g., id.*

13 *See* Fred H. Cate et al., Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines 7 (2013).

information collection and use, including whether the data use raises risks of actual consumer harm.[14] As Commissioner Ohlhausen noted at the 2014 Consumer Electronics show, "the success of the Internet has, in large part, been driven by the freedom to experiment with different business models, the best of which have survived and thrived, even in the face of initial unfamiliarity and unease about the impact on consumers."[15] FPF believes that the success of the Internet of Things will require similar "regulatory humility."[16] FPF looks forward to engaging with the Commission and other stakeholders to support industry as it develops appropriate, flexible standards for the Internet of Things.

Flexibility is particularly important with respect to the concepts of notice and choice. Myriad connected devices will be deployed in industrial contexts or to service infrastructure in ways that do not implicate privacy at all. In fact, "most applications of IoT will have little or nothing to do with consumers and data privacy."[17] Sensors that detect whether a person is present in a potentially hazardous location or that collect information about weight distributions on aircraft, vibrations on bridges or wind turbines, or whether safety equipment is deployed appropriately, likely do not require the implementation of privacy protections. And other implementations of the Internet of Things, as described below, will use consumer information in innocuous or beneficial ways that do not warrant notice and choice.

Even where notice and choice is called for, it will not always be practical in the Internet of Things to address the collection and use of personal information via *traditional* notice and choice mechanisms. As pointed out in our White Paper and previously submitted comments, some connected devices will not have screens or interfaces that readily present privacy notices or allow consumers to select among data practices.[18]

---

14 FPF White Paper, *supra* note 7, at 6. *See also Smart Stores*, Future of Privacy Forum, http://www.futureofprivacy.org/issues/smart-stores/; *Smart Grid*, Future of Privacy Forum, http://www.futureofprivacy.org/issues/smart-grid/. That does not mean, though, that traditional implementations should be abandoned entirely.

15 Remarks of Commissioner Maureen K. Ohlhausen, Consumer Electronics Show, Promoting an Internet of Inclusion: More Things AND More People, at 1 (Jan. 8, 2014), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/promoting-internet-inclusion-more-things-more-people/140107ces-iot.pdf.

16 *See generally id.* at 1-2.

17 Kishore Swaminathan, *Toasters, Refrigerators and the Internet of Things*, Accenture (Mar. 2012), http://www.accenture.com/us-en/outlook/Pages/outlook-journal-2012-toasters-refrigerators-internet-things.aspx.

18 FPF White Paper, *supra* note 7, at 4-5; Prior FPF Comments, *supra* note 8, at 2.

One of the oft-mentioned features of the Internet of Things is that it will involve "frequent, often continuous, data inputs and transmissions from a broad array of connected devices."[19] Individuals may encounter thousands of connected devices on a daily basis. As professors Fred Cate and Viktor Mayer-Schönberger suggest in a recent paper, it is unreasonable to think that consumers will be willing or able to register their preferences regarding data collection and use every time they encounter a new device.[20] Those factors indicate that the traditional model of promoting notice and choice by presenting privacy policies and asking consumers to consent to privacy practices will not always be practical. Moreover, in many cases, user interface designs that help communicate to users that an interaction is "smart" and connected to other actions may be more effective than traditional consent models.[21]

Even where it is practical, notice and choice may not always be necessary to protect consumer privacy. For example, if devices use adequately de-identified data, notice and choice will not be necessary. And as the FTC and the White House have recognized, choice is not required to promote privacy when companies use personally identifiable information for purposes compatible with the context in which the information was collected.[22]

In addition, consumer consent can be inferred reasonably based on the context of collection when personally identifiable information is collected for purposes of fraud prevention, network security, fulfillment, legal compliance, improving performance, first-party marketing, or other important activities. Consumers purchasing connected devices will understand and appreciate that information will be used for purposes such as testing product fixes and developing new service offerings for the devices. Consumer expectations should not, however, be the sole determinants of context. Instead, context should be interpreted broadly enough to allow for the innovative, beneficial, and serendipitous uses of data that the Internet of Things will bring—including uses that may be difficult to predict at the outset.[23]

---

19 *See, e.g.*, Ramirez, *supra* note 8, at 1-2; FPF White Paper, *supra* note 7, at 4; Prior FPF Comments, *supra* note 8, at 5-6.
20 Cate et al., *supra* note 13, at 6-7 (discussing that using notice and choice as the primary mechanism for promoting privacy may result in overwhelming consumers).
21 Prior FPF Comments, *supra* note 8, at 6.
22 *See* FTC, *supra* note 10, at 48; The White House, *supra* note 11, at 15-18.
23 FPF White Paper, *supra* note 7, at 9.

In some circumstances, the information collected and its associated use may be so banal as to not warrant notice and choice at all. Many Internet of Things implementations will not require the integration of privacy protections. For example, a smart TV that learns the volume preferences of particular users and adjusts its volume accordingly should not raise any issues necessitating the presentation of privacy policies and prompts for consent, especially if the information used is not transmitted outside the TV. Consider also the machine-to-machine communications of contextually aware devices. Those devices will react to each other in useful ways (*e.g.*, locks that operate based on the recognition of codes in devices). Companies may create contained information flows for these devices that make notice and choice unnecessary.

In some cases, however, such as when consumers are purchasing connected devices that will collect personally identifiable health information, the presentation of privacy policies will be important to helping consumers make informed choices. Consumers have grown to expect that they will be prompted to read (or be given the opportunity to read and at least acknowledge) privacy policies and to consent to privacy practices in those specific situations. There is no reason to expect this aspect of the privacy framework to be abandoned completely in the Internet of Things.

Even in circumstances where traditional implementations may seem appropriate, however, flexibility is needed. Depending on the types of devices involved and the environments in which they are used, different privacy implementations may be preferable. In some cases, device displays may be available, while in others, consumer profile management portals or online "dashboards" will be feasible.[24] In some circumstances, it may be appropriate to present privacy notices prior to purchase or registration, such as when a consumer is considering whether to buy an Internet-connected health monitoring device. In other circumstances, such as the installation of apps in moving vehicles, it may be more appropriate to provide simple notice of the existence of privacy policies and allow consumers to read those policies after installation.

For all of these reasons, as well as those discussed in our White Paper, FPF proposes the adoption of flexible approaches to implementing the FIPPs as the Internet of Things

24 Prior FPF Comments, *supra* note 8, at 6.

develops. Here are some of the ways in which a context-specific, use-based privacy framework can promote traditional privacy principles:

- **Notice** promotes privacy by providing consumers with relevant information. In our White Paper, we propose that organizations should be transparent about how they will use personally identifiable information. Rather than rigid standards about the presentation and content of privacy disclosures, however, we would like to see the appropriate levels of transparency be determined by the context in which information is collected, including the nature of the data collected and the purposes for which it will be used.[25] For example, if the nature of data use is readily apparent from the context, privacy disclosures are likely unnecessary. The same is true if the collection and use of information is so mundane as to not raise any privacy risks. Other examples will likely arise as new connected devices are designed and deployed.
- **Data minimization** promotes privacy by limiting the amount of personal information in circulation. Traditionally, data minimization has often been implemented by placing strict limits on how much personal information is collected. However, another way to implement data minimization is to promote the use of anonymized, rather than identifiable, data.[26] As the FTC acknowledged in its 2012 privacy report, data that has been reasonably de-identified does not raise significant privacy concerns.[27]
- **Use limitation** is sometimes implemented by requiring that personally identifiable information be used only as specified at the time of collection.[28] Another way to implement this principle, as suggested in our White Paper, is to limit the use of information based on the context in which it is collected—for example, not using the data to make eligibility determinations. In this way, use limitation can be promoted without unduly limiting innovative uses of data by requiring organizations to use data only as expressly specified.[29] *Ex ante* rules on when data use is appropriate are ill-advised.

25 FPF White Paper, *supra* note 7, at 10.
26 *See id.* at 7-9.
27 *See* FTC, *supra* note 10, at 22.
28 *See, e.g.*, Directive 95/46, 1995 O.J. (L 281) 31, art. 6.
29 *See* FPF White Paper, *supra* note 7, at 9.

> Instead, privacy frameworks should be designed to allow flexibility to accommodate serendipitous and innovative uses of data, such as those mentioned in our White Paper.[30]

It is our hope that our White Paper, our prior comments,[31] and the discussion here illustrate that the Internet of Things is not well-suited to a one-size-fits all approach to promoting consumer privacy. As the Internet of Things matures and when circumstances dictate that privacy protections are needed, the myriad types of connected devices and the varied contexts in which those devices will operate will require the implementation of flexible frameworks designed to address evolving privacy issues and consumer preferences. Imposing rigid or universal standards to promote privacy in the Internet of Things would risk unduly limiting innovative uses of data and the corresponding societal benefits,[32] and those standards might not be suited to the privacy risks and consumer preferences that emerge in a mature Internet of Things landscape.

III. Security

Data security may have been the most frequently raised concern during the FTC Workshop. FPF agrees that data security is of outsized importance to the robust development of the Internet of Things and should be a priority for all stakeholders. In our prior comments, we noted that "the Internet of Things will not be able to achieve its full potential unless administrative and technical measures are in place to protect against authorized access or disclosure of data collected by connected devices."[33] The security lapses that led to the FTC's recent enforcement action against TRENDnet illustrate how inadequate security can expose consumers to actual privacy and safety risks.[34] If connected devices do not have security "baked in" from the beginning of the development cycle, there are risks that consumers' personal information will be compromised and

30 *Id.* at 5-6 (noting how United Nations Global Pulse has used mobile phone data to understand socio-economic activity, plan infrastructure, and predict the spread of disease).
31 Prior FPF Comments, *supra* note 8, at 7.
32 This conclusion was also expressed by some of the stakeholders responding to the European Commission's public consultation on Internet of Things governance. European Commission, Directorate-General for Communications Networks, Content and Technology, Report on the Public Consultation of IoT Governance 15 (2013), *available at* http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1746.
33 Prior FPF Comments, *supra* note 8, at 7.
34 *See* Press Release, FTC, Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy, (Sep. 4, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles.

that bad actors will be able to control connected devices without the knowledge or consent of the devices' owners.[35]

Inadequate security presents the greatest risk of actual consumer harm in the Internet of Things. Without adequate security, bad actors may take control of connected devices, pry into intimate spaces, or perpetrate fraud or identity theft. Because inadequate security presents such a tangible risk of causing actual consumer harm, companies must ensure that they devote adequate resources to security before and after their products reach the market.

However, there is already significant attention being paid to the security issues associated with the Internet of Things. At the Workshop, panelists from industry reflected the awareness that without the strictest attention to security, consumer safety may be imperiled and consumer confidence will be lost. In a recent blog post, IBM's Big Data Evangelist, James Kobielus, wrote, "Security is critical to IoT's adoption because we want to make sure we can 'trust' the sensors, actuators, rules engines and other connected componentry we embed in every element of our existence."[36] Kobielus notes that while there is yet no comprehensive solution for Internet of Things security issues, "the [Internet of Things] industry is beginning to address these challenges on many fronts."[37] Already, much work has been done to identify the security requirements that should become integrated into Internet of Things ecosystems, including:

- Emphasizing "security by design" in the development of connected devices;
- Maintaining inventories of connected devices;
- Securing the supply chain from manufacturer to end user and technical support;
- Conducting independent security audits and penetration testing of connected devices;
- Ensuring that connected devices can be updated with security patches;
- Monitoring vulnerability reports and attacks;
- Ensuring that proper access controls are built into connected devices and Internet of Things ecosystems; and

35 *See* Yoshi Kohno, Remarks at FTC Workshop, Internet of Things: Privacy and Security in a Connected World (Nov. 19, 2013) (p. 244 line 20 of transcript), *available at* http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf.
36 James Kobielus, *Securing the Internet of Things: Where Do You Start?*, The Big Data Hub (Dec. 19, 2013), http://www.ibmbigdatahub.com/blog/securing-internet-things-where-do-you-start.
37 *Id.*

- Implementing appropriate de-identification and encryption measures.[38]

Industry's attention to securing the Internet of Things was evidenced on the same day as the Workshop, when Verizon announced the launch of a cloud-based service designed to "authenticate objects and machines" and secure the transmissions between them.[39]

Although Professor Tadoyoshi Kohno described at the Workshop the several-years-old laboratory research that he and other researchers conducted on potential security vulnerabilities in selected connected automobiles, Professor Kohno acknowledged that the "risk to car owners today is incredibly small."[40] The automotive industry, he said, has focused significant resources on the security issues facing connected cars.[41] That observation was reinforced by the presentations of other panelists at the Workshop, demonstrating the seriousness with which industry takes data security in the Internet of Things.

A rigid, one-size-fits-all approach to the data security issues is both unfeasible and counterproductive. As other commenters have noted, there are a variety of industry efforts underway to develop standards for Internet of Things services, including security standards. These standards must be flexible enough to accommodate the evolving array of technologies and services associated with the Internet of Things. Rigid, non-flexible security standards would likely lead to check-box compliance. This *might* be sufficient to address today's security risks. However, as Internet of Things technologies evolve, so too will security vulnerabilities and risks. To address the security risks associated with the Internet of Things, industry will have to monitor incidents and vulnerability reports, and engage in risk-based assessments of security measures on an ongoing basis. Even those who believe that greater attention is required to security in the Internet of Things also believe that "an important level of flexibility" is needed to address

38 *See id.*
39 Press Release, Verizon Launches New Security Suite to Protect the Internet of Things (Nov. 19, 2013), *available at* http://newscenter.verizon.com/corporate/news-articles/2013/11-19-new-security-suite-to-protect-internet/.
40 Yoshi Kohno, Remarks at FTC Workshop, Internet of Things: Privacy and Security in a Connected World (Nov. 19, 2013) (p. 266 lines 6-7 of transcript), *available at* http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf.
41 *Id.* (p. 264 of transcript).

security.[42] The wide range of connected devices and the diversity of environments in which they will be implemented demand that security practices "be framed in functional terms that are agnostic to underlying physical implementations"[43] and address security issues in context.

Consumer demand for secure devices, along with potential FTC enforcement action like the one brought against TRENDnet, should further incentivize companies to remain vigilant and to implement security-by-design policies and procedures.

IV. Data Collection

Another issue frequently raised during the Workshop concerned the comprehensive data collection often associated with the Internet of Things. As Chairwoman Ramirez noted in her opening remarks, the Internet of Things may sometimes involve the collection of vast amounts of data that will enable organizations to develop "deeply personal and startlingly complete" consumer profiles.[44] Companies offering connected devices and services may be able to learn about consumers' health, financial, and other information that consumers reasonably consider to be sensitive.

However, not all connected devices will facilitate the ubiquitous collection of personally identifiable information. Many connected devices will be designed to recognize the presence of other devices or other environmental factors and respond accordingly. Connected clothing may adjust its thickness based on weather reports and body temperature without compiling or transmitting that information.[45] However, some connected devices will be able to facilitate the collection of detailed consumer profiles that could be used to determine medical conditions, creditworthiness, insurability, employment, or similarly significant issues. The value of those profiles to hackers and the possibility that those profiles could be used for inappropriate purpose does raise the risk that consumers could face actual harm.

---

42 *E.g.*, de Leusse *et al.*, *Self Managed Security Cell, a Security Model for the Internet of Things and Services, in Proceedings for the 2009 First International Conference on Advances in Future Internet* 47 (2009), *available at* http://arxiv.org/pdf/1203.0439.pdf .
43 Kobielus, *supra* note 36.
44 Ramirez, *supra* note 8, at 3.
45 *See* NPR Staff, *CES 2014: Toothbrush? Bed? Car? Put Some Internet on It*, NPR (Jan. 6, 2014), *available at* http://www.npr.org/blogs/alltechconsidered/2014/01/06/260189445/ces-2014-toothbrush-bed-car-put-some-internet-on-it.

But these issues are neither new nor unique, and the FTC has addressed them in various contexts. The Internet of Things merely presents a new context in which these concerns arise. In addressing these concerns, it is important to not unduly limit the economic, social, and consumer benefits that the Internet of Things can bring. That is why FPF considers a use-based privacy paradigm to be most appropriate for the Internet of Things. When privacy protections are warranted, the Internet of Things should incorporate approaches that reduce the likelihood that information will be used for inappropriate purposes without establishing obstacles to innovation.

V. Promoting Privacy and Security in the Internet of Things

FPF encourages the FTC to continue engaging with stakeholders to learn about the technologies involved with the Internet of Things, developing business models, existing and emerging self-regulatory structures, and the consumer benefits that are likely to flow from the Internet of Things. As Commissioner Ohlhausen stated at the Workshop, the Commission should develop a full understanding of the Internet of Things ecosystems as well as industry's ongoing initiatives to develop standards for the implementation of connected devices.[46] It is important that the FTC understand the consumer and non-consumer uses of connected devices to ensure that any enforcement activities in the Internet of Things do not unduly impact industrial uses of connected devices, such as monitoring turbines or weight distributions on aircraft. And FPF agrees with Commissioner Ohlhausen that if consumer harms do arise, the Commission "should carefully consider whether existing laws and regulations are sufficient to address them before assuming that new rules are required."[47]

FPF urges the FTC to continue its advocacy of the high-level principles of privacy by design, simplified consumer choice, and transparency while being mindful of the need for flexibility described above. High-level principles are particularly well-suited for the Internet of Things as they allow policies and procedures to be tailored to the nature of connected devices, the environments in which they are used, the purposes for which the information is used, and the evolution of consumer preferences.

---

46 Ohlhausen, *supra* note 8, at 1-2.
47 Remarks of Commissioner Maureen K. Ohlhausen, Consumer Electronics Show, Promoting an Internet of Inclusion: More Things AND More People, at 2 (Jan. 8, 2014), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/promoting-internet-inclusion-more-things-more-people/140107ces-iot.pdf.

Privacy by design is essential to the Internet of Things. "Companies developing new products should build in consumer privacy protections from the outset."[48] The development of privacy and security tools, features, and protections should not be an afterthought. Privacy and security should inform every step of the development cycle, and tools and settings should be easy to use and understand.

Simplified consumer choice can also be integral to the promotion of privacy. Industry should, when warranted, seek to provide reasonable choices over the collection and use of personally identifiable information. As discussed above, context should play an important role in determining whether and how to offer consumer choice mechanisms. But context should not be unduly limited by consumer expectations. The value of the Internet of Things will largely come from rapidly evolving, beneficial uses of data. When considering whether the use of data is appropriate to the context, consideration should instead be given to the likely benefits and the risk, if any, of actual harm.

Transparency can also be vital to the development of the Internet of Things. Industry must ensure that consumers understand how they will benefit from the Internet of Things and see that measures are in place to promote consumer privacy and security.[49] Many companies have already recognized this, and FPF has worked with industry and other stakeholders to develop programs that promote transparency in the world of connected devices.

For the smart grid, FPF worked with stakeholders to develop a privacy seal program for companies providing services to consumers that rely on energy data.[50] The privacy seal program promotes transparency by providing consumers with timely information about how information will be collected and used while providing companies with flexibility as to how implement the privacy principles guiding the program.[51] In October of 2013, FPF was pleased to announce the development of a code of conduct for mobile location analytics ("MLA") companies that track shoppers' locations through stores.[52] The code directs MLA companies to develop privacy notices

48 Ramirez, *supra* note 8, at 3.
49 *See* Prior FPF Comments, *supra* note 8, at 5.
50 *Id.* at 8-11.
51 *Id.* at 10.
52 Press Release, The Future of Privacy Forum and Sen. Schumer Announce Important Agreement to Ensure Consumers Have Opportunity to "Opt-Out" Before Stores Can Track Their Movement via Their Mobile Devices

that inform consumers about how information will be collected, used, and stored, and MLA companies are to work with retailers to develop signage that will alert consumers to the use of tracking technologies and direct consumers to where they can obtain more information.[53] FPF's experiences with these programs indicate that industry groups are willing to develop robust codes of conduct and other programs that promote transparency and are tailored to the identifiability of the information involved and the varied environments in which technologies will be implemented.

Along with promoting privacy by design, simplified consumer choice, and transparency, the FTC will continue to have the ability to shape privacy and security practices by using its Section 5 authority to take action against bad actors. The FTC's enforcement actions and policy reports have shaped leading practices in the mobile app ecosystem and other areas, and FPF believes that the same can be true for the Internet of Things. As a critical part of this mission, we encourage the FTC to consider industry's need for flexibility to create innovative products and services that will have benefits for consumers, as well as society at large.

VI. Conclusion

FPF appreciates the opportunity to engage with the Commission on the Internet of Things, and we look forward to our further engagement and collaboration. The Internet of Things represents an important part of consumers' technology future. So long as thoughtful attention is given to privacy and security issues, that future promises to be bright.

Respectfully submitted,

Jules Polonetsky
Co-Chair and Director

Christopher Wolf
Founder and Co-Chair

FUTURE OF PRIVACY FORUM
919 18th Street NW
Washington, DC 200036

(Oct. 22, 2013), *available at* http://www.futureofprivacy.org/2013/10/22/schumer-and-tech-companies-announce-important-agreement-to-ensure-consumers-have-opportunity-to-opt-out-before-stores-can-track-their-movement-via-their-cell-phones/.

53 Mobile Location Analytics Code of Conduct (2013), *available at* http://www.futureofprivacy.org/wp-content/uploads/10.22.13-FINAL-MLA-Code.pdf.

Appendix A

An Updated Privacy Paradigm for the "Internet of Things"

By Christopher Wolf and Jules Polonetsky
Co-Chairs, Future of Privacy Forum

November 19, 2013

The Future of Privacy Forum is a think tank whose mission is to advance privacy for people in practical ways that allow for innovation and responsible uses of data. The FPF Advisory Board includes representatives of business, privacy scholars and consumer advocates. www.futureofprivacy.org

Introduction

The "Internet of Things" refers to the information networks comprised of sensors and other technologies embedded in physical objects and linked via wired and wireless networks. Cisco estimates that there are nearly 11 billion connected objects in the world.[1] By 2020, there may be more than 200 billion connected devices.[2] As the Internet of Things matures, more and more everyday objects will "wake up," become aware of their environments, communicate the information that they collect, and receive information from outside sources. This will likely generate substantial economic and social benefits, including improved health care, increased public and personal safety,

[1] *Connections Counter: The Internet of Everything in Motion*, Cisco Newsroom, http://newsroom.cisco.com/feature-content?articleId=1208342 (last visited Oct. 29, 2013).

[2] *See* Press Release, International Data Corporation, *The Internet of Things Is Poised to Change Everything, Says IDC* (Oct. 3, 2013), *available at* http://www.idc.com/getdoc.jsp?containerId=prUS24366813.

efficient use of resources, business innovations, and more. This paper examines the need for an updated, forward-looking privacy paradigm for the Internet of Things.

The Current Privacy Paradigm Is Not Practical for the Internet of Things

Along with these potential benefits, the Internet of Things gives rise to debate over privacy and security concerns. In some cases, existing privacy concerns are heightened by the increased data interaction with newly interconnected objects. Therefore, the question is: *How do we account for privacy in the Internet of Things?*

Traditionally, privacy concerns have been addressed by application of the Fair Information Practice Principles ("FIPPs"), which address the treatment of personal information. In 1973, the United States Department of Health, Education, and Welfare offered the first comprehensive articulation of the FIPPs.[3] The FIPPs have since been embodied in U.S. and European Union privacy laws and serve as the basis for a range of privacy frameworks established by legislatures, government agencies, and international bodies.[4] The Organization for Economic Cooperation and Development developed one of the more influential variations of the FIPPs in its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("Guidelines").[5] The Guidelines, which were adopted in 1980 and revised this year, are intended to "address concerns arising from the increased use of personal data and the risk to global

[3] FTC, Privacy Online: A Report to Congress 48 n.27 (1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf.

[4] *See e.g.*, The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (2012); FTC, Protecting Consumer Privacy in an Era of Rapid Change 22 (2012). *See generally* John W. Kropf, *Independence Day: How to Move the Global Privacy Dialogue Forward*, Bloomberg BNA Privacy & Security Law Report (Jan 12, 2009)

[5] *See* Kropf, *supra* note 4.

economies resulting from restrictions to the flow of information across boundaries."[6] Since then, the FIPPs have been presented in different ways with different emphases.[7]

In their various formulations, the FIPPs establish core principles guiding the collection, use, and disclosure of data.[8] Some of the more important FIPPs are 1) Notice- individuals should be provided with timely notice of how their data will be collected, used, and disclosed; 2) Choice- individuals should be given choices about whether and how their data will be used; 3) Data Minimization- organizations should seek to limit the amount of personal data they collect and that might be retained; 4) Purpose Specification- the purposes for which personal data are collected should be specified prior to or at the time of collection; and 5) Use Limitation- personal data should only be used for those purposes specified prior to or at the time of collection.[9]

Privacy Challenges Presented by the Internet of Things Cannot be Solved by Simple Application of the FIPPs.

The FIPPs generally have been thought of as establishing high-level guidelines for the implementation of specific codes of practice.[10] They do not establish a specific set of rules prescribing how organizations must go about promoting privacy in all contexts. The FIPPs of notice and choice are often implemented in ways that are not well-suited for the Internet of Things, such as through the posting of privacy policies and the use of

---

6 OECD, OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data 19 (2013), *available at* http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

7 *See supra* note 4; Edith Ramirez, The Privacy Challenges of Big Data: A View from the Lifeguard's Chair, Keynote Address by FTC Chairwoman Edith Ramirez, Technology Policy Institute Aspen Forum (Aug. 19, 2013), *available at* http://www.ftc.gov/speeches/ramirez/130819bigdataaspen.pdf.

8 *See, e.g.*, *id.* at 13-14; The White House, *supra* note 4, at 10.

9 *See, e.g.*, OECD, *supra* note 6, at 14; The White House, *supra* note 4, at 11-19, 21.

10 *E.g.,* The White House, *supra* note 4, at 16 n.21.

click-through consent mechanisms. Many connected devices, such as traffic sensors embedded in roadways, will not be equipped with interactive screens or other user

interfaces. When the Internet of Things matures, it is likely that most connected devices will be invisible to us (*i.e.*, we will not interact directly with them frequently, if at all). Moreover, the individual owning or registering a device may lend that device to others. In those situations, the person operating the device may not have had the opportunity to provide consent to data collection. Although technological solutions may be developed to facilitate notice and choice options, it would be impractical to premise data collection and use in the Internet of Things on traditional notice and choice implementations.

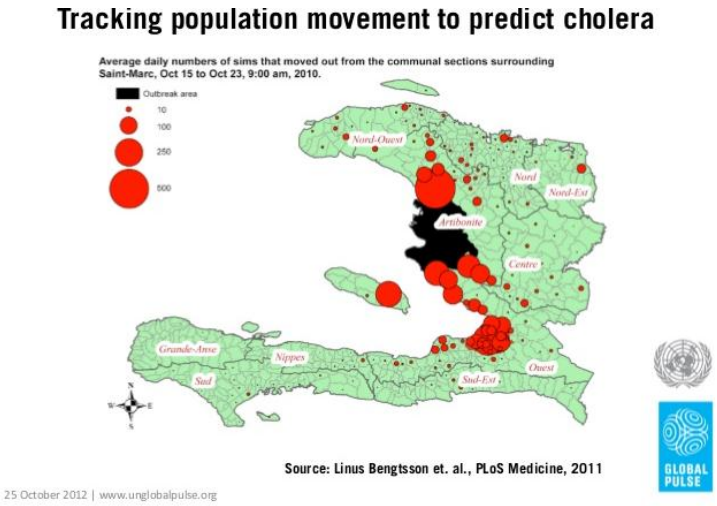
The Internet of Things relies on frequent, often continuous, data inputs and transmissions from a broad array of connected devices. If the only way to authorize the collection of personal data were based on traditional notice and choice, individuals would be prompted to consent to data collection and use each time they bumped into new connected devices. That could occur hundreds or thousands of times a day. Not only would that substantially slow the data transmissions underlying the Internet of Things, it would be incredibly burdensome for individuals and could hinder the development of innovative new technologies.

It is unrealistic to expect that individuals will be willing or able to effectively register their informed preferences in a world where they are regularly prompted to read and accept notices of complex data collection, use, and sharing practices. Individuals may end up blindly accepting data practices rather than having to endure reading yet one more

privacy disclosure.[11] Instead of protecting privacy, strict adherence to traditional notice and choice principles may drive individuals to give up.

Purpose specification, data minimization, and use limitation also present problems for the Internet of Things. As mentioned before, those principles require organizations to specify the purposes for which they will use the data they collect, collect only that data needed to achieve those ends, and use the data only for specified purposes. That risks unduly limiting the development of new services and the discoveries that may follow from valuable research.

Consider the innovations pioneered by the United Nations Global Pulse that are enabled by the analysis of mobile phone data. Global Pulse has helped us understand mobility, social interaction and economic activity.[12] By analyzing mobile interactions, UN researchers were able to examine the post-earthquake population migration caused by the Haiti earthquake.



[11] *See generally* Fred H. Cate & Viktor Mayer-Schönberger, Notice and Consent in a World of Big Data, Int'l Data Privacy Law, Vol. 3, No. 2 (2013).

[12] Robert Kirkpatrick, Beyond Targeted Ads: Big Data for a Better World (2012), *available at* http://www.slideshare.net/unglobalpulse/strata-14934034.

Global Pulse has been able to map the areas in Kenya where Malaria was likely to spread and assess how well Mexico was combating the H1N1 virus. They were also able to better understand socio-economic activity in a number of countries, as well as to help plan road infrastructure and analyze traffic patterns.

Across the US, utilities have installed smart meters, seeking to help residents manage power use more effectively and benefit the environment. Utilities will be able to learn how to adapt and manage their systems—thereby securing the stability and efficiency of the smart grid—only by understanding how residents change their usage patterns. As electric vehicles increasingly are charged at home, understanding how and when drivers come home and plug-in their vehicles will be needed to ensure that the grid can adapt to changing patterns, lest we risk overburdening the system at the end of each evening commute. In the course of managing the smart grid, we are likely to uncover a host of surprising uses for which we can use data about power usage. We may discover that that data can be used to promote health or identify the need for new transportation, entertainment, or food storage technologies.

You cannot specify what you cannot imagine. If data can be processed only in accord with specified purposes, we risk losing out on the unimagined possibilities that the Internet of Things may provide. Our challenge is to allow practices that will support progress, and provide appropriate controls over those practices that should be forestalled or constrained by appropriate consent.[13]

[13] For example, determining the balance between the benefits of new uses and the attendant risks may in some instances require more sophisticated privacy impact assessments that can analyze the impact of risks or harms and assess the potential benefits for individuals and society. *See* Jules Polonetsky & Omer

The inadequacy of traditional privacy practices in the Internet of Things era is not entirely surprising. We tend to view privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[14] But the revolutionary impact of the Internet of Things derives largely from its reliance on myriad and continuous communications. To ask individuals to protect their privacy by managing those communications would be akin to telling Sisyphus that he can rest as soon as he gets that rock to settle atop the hill.

A Use-Focused Privacy Paradigm Is Well-Suited for the Internet of Things

Rather than focusing on how information is collected and communicated, we should rely on how personally identifiable information is used. The following proposals reflect how this can be done.

Use anonymized data when practical. When organizations use adequately anonymized data sets, their use of that data should not be restricted under privacy laws or regulations. As noted by the Federal Trade Commission in its 2012 privacy report, further privacy assurances can be obtained when organizations publicly commit to not re-identify data and when organizations contractually require the third parties to which they send anonymized data to not attempt re-identification.[15] Anonymizing personal information decreases the risks that personally identifiable information will be used for

---

Tene, Privacy and Big Data: Making Ends Meet, 66 Stan. L. Rev. Online 25, 26-27 (2013), http://www.stanfordlawreview.org/online/privacy-and-big-data/privacy-and-big-data.

[14] Alan F. Westin, Privacy and Freedom 7 (1967).

[15] FTC, Protecting Consumer Privacy in an Era of Rapid Change 22 (2012).

unauthorized, malicious, or otherwise harmful purposes.[16] Properly anonymized data are highly unlikely to have any impact on individuals and do not implicate privacy concerns.

Although there have been some reports of researchers who were able to re-identify information from supposedly anonymized data sets, it would be a mistake, however, to conclude that it is always easy to re-identify data or that anonymization is not a useful, privacy-protective practice. In 2009, a group of experts attempted to re-identify approximately 15,000 patient records that had been de-identified under the standards of the Health Insurance Portability and Accountability Act ("HIPAA"). They used commercial data sources to re-identify the data and were able to identify only .013% of the individuals.[17] When data sets are anonymized properly, re-identification is no easy task.[18] When anonymized data sets are kept securely in house with a strong commitment and internal checks to prevent re-identifying the data, then anonymization serves as a strong protection to address privacy concerns.

Whether a specific anonymization practice is appropriate will depend on the circumstances.[19] When anonymizing data, organizations should assess the risks that the data could be re-identified given the nature of the data, the context in which the data will be used, and the resources available to those with access to the data.

---

[16] *See* Ann Cavoukian & Khaled El Emam, Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy 4 (2011).

[17] Deborah Lafkey, *The Safe Harbor Method of De-Identification: An Empirical Test*, ONC Presentation, October 8, 2009, *available at* http://www.ehcca.com/presentations/HIPAAWest4/lafky_2.pdf.

[18] Cavoukian & El Emam, *supra* note 16, at 7.

[19] For example, gender is not an identifying characteristic if every member of a large data set is female. However, if there is only one woman in data set, using gender in the data set will facilitate identification of her.

Organizations that are inexperienced with anonymization should consider implementing third-party testing to determine the likelihood of re-identification.

With robust anonymization practices in place, organizations will be able to use information as needed to realize the mature development of the Internet of Things and spur tomorrow's headline technologies while promoting individual privacy.

Respect the context in which personally identifiable information is collected. This principle is often interpreted to mean that personally identifiable information should be used only in the ways that individuals would expect given the context of the collection. Consumers expect that companies will share personally identifiable information with other companies to fulfill orders and that companies will use personal information to engage in first-party marketing. When personally identifiable information is used in those ways or in others that individuals would reasonably expect, there is no privacy violation.

However, respect for context should not focus solely on what individuals would expect; there may be unexpected new uses that turn out to be valuable societal advances or important new ways to use a product or service. Consider a company that collects personal fitness information from wearable sensors that track sleep, steps taken, pulse or weight. Analysis of such data, collected originally only to report basic details back to users, may yield unanticipated health insights that could be provided individually to users or used in the aggregate to advance medical knowledge. Rigidly and narrowly specifying context could trap knowledge that is available and critical to progress.

Be transparent about data use. To complement the respect for context principle, organizations should be transparent about the purposes for which they will use personally identifiable information. Even if organizations cannot predict how they will use personally identifiable information in the Internet of Things, they can inform individuals that they will use such information to improve products, conduct research, or increase security measures. Organizations making decisions that affect individuals could, subject to protecting their intellectual property, disclose the high-level criteria used when making those decisions. Insurance companies, for instance, could disclose that they determine premiums solely by reviewing driving habits, location, driving history, and other permissible data categories. The insurance companies could clarify that factors such as ethnicity, sexual orientation, and political preferences are not factored into premium determinations.

The required levels of transparency and limitations to which data may be used in a given context should, however, be tailored to the level of identifiability of data, with adequately anonymized data being subject to fewer limits or restrictions.

Automated accountability mechanisms can be designed to determine how personally identifiable information is used and whether the uses conform to established policies. As data flows become more and more complex, it will become more and more difficult for individuals to monitor and enforce privacy compliance. To support privacy compliance, organizations should develop and implement automated systems that can monitor and assess the myriad uses and transmissions of personally identifiable information. Professor Hal Abelson at MIT has proposed that information be tagged with its provenance and logs of transfers and uses. Automated accountability mechanisms

could monitor data usage and determine whether the uses comply with machine readable policies.[20] When improper uses are identified (*e.g.*, credit is denied after viewing someone's political affiliation), accountability mechanisms could notify appropriate parties and trigger appropriate actions.

Develop Codes of Conduct. As the Internet of Things becomes more ubiquitous, parents will want to control what can be done with information collected from devices associated with their children. Others may want to indicate their preferences about how third-party connected devices will communicate with them. Self-regulatory codes of conduct will be the most effective means to honor these preferences and others in the rapidly evolving landscape of the Internet of Things. Codes of conduct could establish frameworks that enable individuals to associate usage preferences with their connected devices. These preferences would indicate to other devices how information collected from individuals' devices may be used. Preferences could serve as inputs for the accountability mechanisms discussed above, and robust codes of conduct (perhaps supported by audits of accountability mechanisms) could serve to establish accountability.

It's not too early to start, as FPF has pioneered codes of conduct for smart home devices and for smart stores and is coordinating a working group of connected car leaders.

Provide individuals with reasonable access to personally identifiable information. Businesses and other organizations could allow individuals reasonable access to and

[20] Hal Abelson, Information Accountability as the Foundation of 21st Century Privacy Protection (2013), *available at* http://kit.mit.edu/sites/default/files/documents/Abelson_MIT_KIT_2013_Conference.pdf.

use of their personally identifiable information. This will likely enhance consumer engagement with and support of the Internet of Things. One way to provide reasonable access would be to offer tools that allow users to add, tailor, or featurize data, perhaps by allowing access via third-party application programming interfaces. The more effectively that data is anonymized, the less the need and the ability to provide detailed access.

Conclusion

Time tested privacy principles will continue to have relevance for the Internet of Things, but policymakers will need to be flexible and creative in applying these principles to new technologies. As they evaluate their role, and that of industry, in protecting personal privacy and ensuring data security in the world of the Internet of Things, a rigid application of the current privacy paradigm is not practical or appropriate. Thus, we respectfully urge consideration of the updated privacy paradigm we have proposed for the Internet of Things.