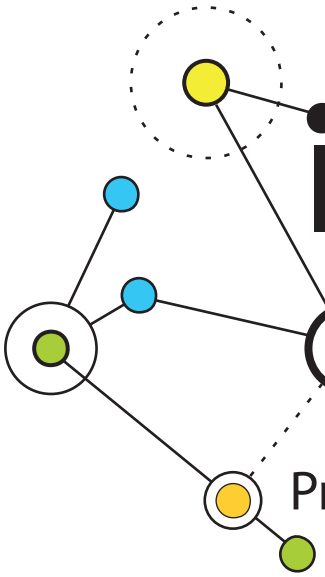
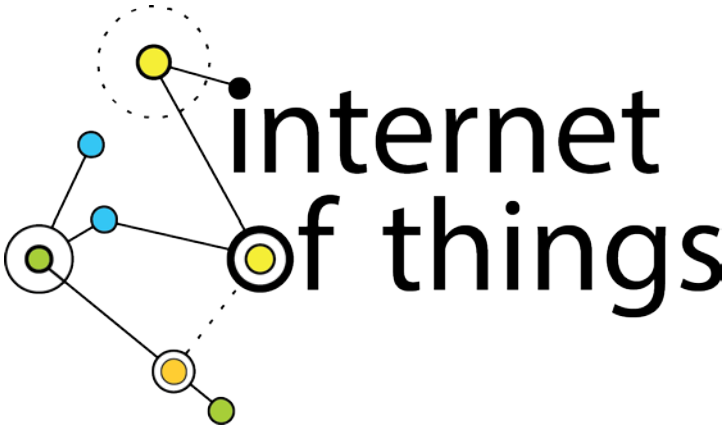


internet of things

Privacy & Security in a Connected World

FTC Staff Report

JANUARY 2015



FTC Staff Report
January 2015

Table of Contents

Executive Summary

The Internet of Things ("IoT") refers to the ability of everyday objects to connect to the Internet and to send and receive data. It includes, for example, Internet-connected cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and bracelets that share with your friends how far you have biked or run during the day.

Six years ago, for the first time, the number of "things" connected to the Internet surpassed the number of people. Yet we are still at the beginning of this technology trend. Experts estimate that, as of this year, there will be 25 billion connected devices, and by 2020, 50 billion.

Given these developments, the FTC hosted a workshop on November 19, 2013 – titled *The Internet of Things: Privacy and Security in a Connected World*. This report summarizes the workshop and provides staff's recommendations in this area.[1] Consistent with the FTC's mission to protect consumers in the commercial sphere and the focus of the workshop, our discussion is limited to IoT devices that are sold to or used by consumers. Accordingly, the report does not discuss devices sold in a business-to-business context, nor does it address broader machine-to-machine communications that enable businesses to track inventory, functionality, or efficiency.

Workshop participants discussed benefits and risks associated with the IoT. As to benefits, they provided numerous examples, many of which are already in use. In the health arena, connected medical devices can allow consumers with serious medical conditions to work

[1] Commissioner Wright dissents from the issuance of this Staff Report. His concerns are explained in his separate dissenting statement.

with their physicians to manage their diseases. In the home, smart meters can enable energy providers to analyze consumer energy use, identify issues with home appliances, and enable consumers to be more energy-conscious. On the road, sensors on a car can notify drivers of dangerous road conditions, and software updates can occur wirelessly, obviating the need for consumers to visit the dealership. Participants generally agreed that the IoT will offer numerous other, and potentially revolutionary, benefits to consumers.

As to risks, participants noted that the IoT presents a variety of potential security risks that could be exploited to harm consumers by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating risks to personal safety. Participants also noted that privacy risks may flow from the collection of personal information, habits, locations, and physical conditions over time. In particular, some panelists noted that companies might use this data to make credit, insurance, and employment decisions. Others noted that perceived risks to privacy and security, even if not realized, could undermine the consumer confidence necessary for the technologies to meet their full potential, and may result in less widespread adoption.

In addition, workshop participants debated how the long-standing Fair Information Practice Principles ("FIPPs"), which include such principles as notice, choice, access, accuracy, data minimization, security, and accountability, should apply to the IoT space. The main discussions at the workshop focused on four FIPPs in particular: security, data minimization, notice, and choice. Participants also discussed how use-based approaches could help protect consumer privacy.

1. Security

There appeared to be widespread agreement that companies developing IoT products should implement reasonable security. Of course, what constitutes reasonable security for a given device will depend on a number of factors, including the amount and sensitivity of data collected and the costs of remedying the security vulnerabilities. Commission staff encourages companies to consider adopting the best practices highlighted by workshop participants, including those described below.

First, companies should build security into their devices at the outset, rather than as an afterthought. As part of the security by design process, companies should consider: (1) conducting a privacy or security risk assessment; (2) minimizing the data they collect and retain; and (3) testing their security measures before launching their products. Second, with respect to personnel practices, companies should train all employees about good security, and ensure that security issues are addressed at the appropriate level of responsibility within the organization. Third, companies should retain service providers that are capable of maintaining reasonable security and provide reasonable oversight for these service providers. Fourth, when companies identify significant risks within their systems, they should implement a defense-in-depth approach, in which they consider implementing security measures at several levels. Fifth, companies should consider implementing reasonable access control measures to limit the ability of an unauthorized person to access a consumer's device, data, or even the consumer's network. Finally, companies should continue to monitor products throughout the life cycle and, to the extent feasible, patch known vulnerabilities.

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. Although some participants expressed concern that requiring data minimization could curtail innovative uses of data, staff agrees with the participants who stated that companies should consider reasonably limiting their collection and retention of consumer data.

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 such an event. Second, if a company collects and 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.

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's recommendation on data minimization is a flexible one that gives companies many options. 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 de-identify the data they collect. 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.

3. Notice and Choice

The Commission staff believes that consumer choice continues to play an important role in the IoT. Some participants suggested that offering notice and choice is challenging in the IoT because of the ubiquity of data collection and the practical obstacles to providing information without a user interface. However, staff believes that providing notice and choice remains important.

This does not mean that every data collection requires choice. The Commission has recognized that providing choices for every instance of data collection is not necessary to protect privacy. In its 2012 Privacy Report, which set forth recommended best practices, the Commission stated that companies should not be compelled to provide choice before collecting and using consumer data for practices that are consistent with the context of a transaction or the company's relationship with the consumer. Indeed, because these data uses are generally consistent with consumers' reasonable expectations, the cost to consumers and businesses of providing notice and choice likely outweighs the benefits. This principle applies equally to the Internet of Things.

Staff acknowledges the practical difficulty of providing choice when there is no consumer interface and recognizes that there is no one-size-fits-all approach. Some options include developing video tutorials, affixing QR codes on devices, and providing choices at point of sale, within set-up wizards, or in a privacy dashboard. Whatever approach a company decides to take, the privacy choices it offers should be clear and prominent, and not buried within lengthy documents. In addition, companies may want to consider using a combination of approaches.

Some participants expressed concern that even if companies provide consumers with choices only in those instances where the collection or use is inconsistent with context, such an

approach could restrict unexpected new uses of data with potential societal benefits. These participants urged that use limitations be considered as a supplement to, or in lieu of, notice and choice. With a use-based approach, legislators, regulators, self-regulatory bodies, or individual companies would set "permissible" and "impermissible" uses of certain consumer data.

Recognizing concerns that a notice and choice approach could restrict beneficial new uses of data, staff has incorporated certain elements of the use-based model into its approach. For instance, the idea of choices being keyed to context takes into account how the data will be used: if a use is consistent with the context of the interaction – in other words, it is an expected use – then a company need not offer a choice to the consumer. For uses that would be inconsistent with the context of the interaction (*i.e.*, unexpected), companies should offer clear and conspicuous choices. In addition, if a company collects a consumer's data and de-identifies that data immediately and effectively, it need not offer choices to consumers about this collection. Furthermore, the Commission protects privacy through a use-based approach, in some instances. For example, it enforces the Fair Credit Reporting Act, which restricts the permissible uses of consumer credit report information under certain circumstances. The Commission also applies its unfairness authority to challenge certain harmful uses of consumer data.

Staff has concerns, however, about adopting a pure use-based model for the Internet of Things. First, because use-based limitations are not comprehensively articulated in legislation, rules, or widely-adopted codes of conduct, it is unclear who would decide which additional uses are beneficial or harmful. Second, use limitations alone do not address the privacy and security

risks created by expansive data collection and retention. Finally, a pure use-based model would not take into account consumer concerns about the collection of sensitive information.[2]

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

4. Legislation

Participants also discussed whether legislation over the IoT is appropriate, with some participants supporting legislation, and others opposing it. Commission staff agrees with those commenters who stated that there is great potential for innovation in this area, and that IoT-specific legislation at this stage would be premature. Staff also agrees that development of self-regulatory programs designed for particular industries would be helpful as a means to encourage the adoption of privacy- and security-sensitive practices.

However, in light of the ongoing threats to data security and the risk that emerging IoT technologies might amplify these threats, staff reiterates the Commission's previous recommendation for Congress to enact strong, flexible, and technology-neutral federal legislation to strengthen its existing data security enforcement tools and to provide notification to consumers when there is a security breach. General data security legislation should protect against unauthorized access to both personal information and device functionality itself. For

[2] In addition to collecting sensitive information outright, companies might create sensitive information about consumers by making inferences from other data that they or others have already collected. A use-based model might not address, or provide meaningful notice about, sensitive inferences. The extent to which a use-based model limits or prohibits sensitive inferences will depend on how the model defines harms and benefits and how it balances the two, among other factors.

example, if a pacemaker is not properly secured, the concern is not merely that health information could be compromised, but also that a person wearing it could be seriously harmed.

In addition, the pervasiveness of information collection and use that the IoT makes possible reinforces the need for baseline privacy standards, which the Commission previously recommended in its 2012 privacy report. Although the Commission currently has authority to take action against some IoT-related practices, it cannot mandate certain basic privacy protections – such as privacy disclosures or consumer choice – absent a specific showing of deception or unfairness. Commission staff thus again recommends that Congress enact broad-based (as opposed to IoT-specific) privacy legislation. Such legislation should be flexible and technology-neutral, while also providing clear rules of the road for companies about such issues as how to provide choices to consumers about data collection and use practices.[3]

In the meantime, we will continue to use our existing tools to ensure that IoT companies continue to consider security and privacy issues as they develop new devices. Specifically, we will engage in the following initiatives:

- **Law enforcement:**
  The Commission enforces the FTC Act, the FCRA, the health breach notification provisions of the HI-TECH Act, the Children's Online Privacy Protection Act, and other laws that might apply to the IoT. Where appropriate, staff will recommend that the Commission use its authority to take action against any actors it has reason to believe are in violation of these laws.

- **Consumer and business education:**
  The Commission staff will develop new consumer and business education materials in this area.

[3] Commissioner Ohlhausen does not agree with the recommendation for baseline privacy legislation. *See infra* note 191.

- **Participation in multi-stakeholder groups:**
  Currently, Commission staff is participating in multi-stakeholder groups that are considering guidelines related to the Internet of Things, including on facial recognition and smart meters. Even in the absence of legislation, these efforts can result in best practices for companies developing connected devices, which can significantly benefit consumers.

- **Advocacy:**
  Finally, where appropriate, the Commission staff will look for advocacy opportunities with other agencies, state legislatures, and courts to promote protections in this area.

Background

Technology is quickly changing the way we interact with the world around us. Today, companies are developing products for the consumer market that would have been unimaginable a decade ago: Internet-connected cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and bracelets that share with your friends how far you have biked or run during the day. These are all examples of the Internet of Things ("IoT"), an interconnected environment where all manner of objects have a digital presence and the ability to communicate with other objects and people. The IoT explosion is already around us, in the form of wearable computers, smart health trackers, connected smoke detectors and light bulbs, and essentially any other Internet-connected device that isn't a mobile phone, tablet, or traditional computer.

Six years ago, for the first time, the number of "things" connected to the Internet surpassed the number of people.[1] Yet we are still at the beginning of this technology trend. Experts estimate that, as of this year, there will be 25 billion connected devices, and by 2020, 50 billion.[2] Some estimate that by 2020, 90% of consumer cars will have an Internet connection, up from less than 10 percent in 2013.[3] Three and one-half billion sensors already are in the

[1] DAVE EVANS, CISCO INTERNET BUS. SOLUTIONS GRP., THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING 3 (2011), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. These estimates include all types of connected devices, not just those aimed at the consumer market.

[2] *Id*.

[3] TELEFONICA, CONNECTED CAR INDUSTRY REPORT 2013 9 (2013), *available at* http://websrvc.net/2013/telefonica/Telefonica%20Digital_Connected_Car2013_Full_Report_English.pdf.

marketplace,[4] and some experts expect that number to increase to trillions within the next decade.[5] All of these connected machines mean much more data will be generated: globally, by 2018, mobile data traffic will exceed fifteen exabytes – about 15 quintillion bytes – each month.[6] By comparison, according to one estimate, an exabyte of storage could contain 50,000 years' worth of DVD-quality video.[7]

These new developments are expected to bring enormous benefits to consumers. Connected health devices will allow consumers with serious health conditions to work with their physicians to manage their diseases. Home automation systems will enable consumers to turn off the burglar alarm, play music, and warm up dinner right before they get home from work. Connected cars will notify first responders in the event of an accident. And the Internet of Things may bring benefits that we cannot predict.

However, these connected devices also will collect, transmit, store, and potentially share vast amounts of consumer data, some of it highly personal. Given the rise in the number and types of connected devices already or soon to be on the market, the Federal Trade Commission ("FTC" or "Commission") announced in April 2013 that it would host a workshop on the privacy and security issues associated with such devices and requested public input about the issues to

---

[4] *See* Stanford Univ., *TSensors Summit™ for Trillion Sensor Roadmap* 1 (Oct. 23-25, 2013), *available at* http://tsensorssummit.org/Resources/Why%20TSensors%20Roadmap.pdf.

[5] *Id*.

[6] CISCO, CISCO VISUAL NETWORKING INDEX: GLOBAL MOBILE DATA TRAFFIC FORECAST UPDATE, 2013–2018 3 (2014), *available at* http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf.

[7] University of Bristol, Exabyte Informatics, *available at* http://www.bris.ac.uk/research/themes/exabyte-informatics.html.

consider.[8] In response to the request for comment, staff received twenty-nine public comments[9] from a variety of consumer advocacy groups, academics, and industry representatives. The workshop – titled *The Internet of Things: Privacy and Security in a Connected World* – took place on November 19, 2013, and featured panels of academics, researchers, consumer advocates, and representatives from government and industry.[10]

The workshop consisted of four panels,[11] each of which focused on a different aspect of the IoT.[12] The first panel, "The Smart Home,"[13] looked at an array of connected devices, such as home automation systems and smart appliances. The second panel, "Connected Health and Fitness,"[14] examined the growth of increasingly connected medical devices and health and fitness products, ranging from casual wearable fitness devices to connected insulin pumps. The third panel, "Connected Cars,"[15] discussed the different technologies involved with connected

---

[8] Press Release, FTC, FTC Seeks Input on Privacy and Security Implications of the Internet of Things (Apr. 17, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/04/ftc-seeks-input-privacy-and-security-implications-internet-things.

[9] Pre-workshop comments ("#484 cmt.") are available at http://www.ftc.gov/policy/public-comments/initiative-484.

[10] For a description of the workshop, *see* http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world.

[11] In addition to the four panels, workshop speakers included Keith Marzullo of the National Science Foundation ("Marzullo"), who gave an overview of the IoT space (Transcript of Workshop at 15-34); Carolyn Nguyen ("Nguyen") of Microsoft Corp., who discussed contextual privacy and its implications for the IoT (Transcript of Workshop at 35-51); and Vinton "Vint" Cerf ("Cerf") of Google Inc., who gave the workshop's Keynote Address (Transcript of Workshop at 118-153).

[12] A complete transcript of the proceeding is available at http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf. Videos of the workshop also are available at http://www.ftc.gov/news-events/audio-video/ftc-events.

[13] Transcript of Workshop at 52-115.

[14] *Id.* at 164-234.

[15] *Id.* at 235-291.

cars, including Event Data Recorders ("EDRs")[16] and other vehicle "telematics," a term that refers to data collection, transmission, and processing technologies for use in vehicles. Finally, the fourth panel, "Privacy and Security in a Connected World,"[17] discussed the broader privacy and security issues raised by the IoT.

Following the workshop, the Commission invited comments on the issues raised by the panels.[18] In response, staff received seventeen public comments from private citizens, trade organizations, and privacy advocates.[19]

This report summarizes the workshop and provides staff's recommendations in this area. Section II of this report discusses how we define the "Internet of Things." Section III describes some of the benefits and risks of the new technologies that are part of the IoT phenomenon. Section IV examines the application of existing privacy principles to these new technologies, and Section V addresses whether legislation would be appropriate in this area. Sections IV and V begin by discussing the views of written commenters and workshop speakers (collectively, "participants"), and then set forth staff recommendations. These recommendations focus on the types of products and services consumers are likely to encounter today and in the foreseeable future. We look forward to continuing to explore privacy issues as new IoT technologies come to market.

---

[16] An EDR is "a device or function in a vehicle that records the vehicle's dynamic time-series data during the time period just prior to a crash event (*e.g.*, vehicle speed vs. time) or during a crash event . . . intended for retrieval after the crash event." 49 C.F.R. § 563.5.

[17] Transcript of Workshop at 292-364.

[18] Press Release, FTC, FTC Seeks Comment on Issues Raised at Internet of Things Workshop (Dec. 11, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/12/ftc-seeks-comment-issues-raised-internet-things-workshop.

[19] Post-workshop comments ("#510 cmt.") are available at http://www.ftc.gov/policy/public-comments/initiative-510.

What is the "Internet of Things"?

Although the term "Internet of Things" first appeared in the literature in 2005,[20] there is still no widely accepted definition.[21] One participant described the IoT as the connection of "physical objects to the Internet and to each other through small, embedded sensors and wired and wireless technologies, creating an ecosystem of ubiquitous computing."[22] Another participant described it as including "embedded intelligence" in individual items that can detect changes in their physical state.[23] Yet another participant, noting the lack of an agreed-upon definition of the IoT, observed, "[w]hat all definitions of IoT have in common is that they focus on how computers, sensors, and objects interact with one another and process data."[24]

The IoT includes consumer-facing devices, as well as products and services that are not consumer-facing, such as devices designed for businesses to enable automated communications between machines. For example, the term IoT can include the type of Radio Frequency Identification ("RFID") tags that businesses place on products in stores to monitor inventory; sensor networks to monitor electricity use in hotels; and Internet-connected jet engines and drills on oil rigs. Moreover, the "things" in the IoT generally do not include desktop or laptop computers and their close analogs, such as smartphones and tablets, although these devices are often employed to control or communicate with other "things."

---

[20] *See* Remarks of Marzullo, Transcript of Workshop at 19.

[21] *See Comment of ARM/AMD*, #510 cmt. #00018 at 1.

[22] *Comment of Consumer Elec. Ass'n*, #484 cmt. #00027 at 1.

[23] Remarks of Marzullo, Transcript of Workshop at 19.

[24] *Comment of Ctr. for Democracy & Tech.*, #484 cmt. #00028 at 3.

For purposes of this report, we use the term IoT to refer to "things" such as devices or sensors – other than computers, smartphones, or tablets – that connect, communicate or transmit information with or between each other through the Internet. Consistent with the FTC's mission to protect consumers in the commercial sphere, our discussion of IoT is limited to such devices that are sold to or used by consumers. Accordingly, the report does not discuss devices sold in a business-to-business context, such as sensors in hotel or airport networks; nor does it discuss broader machine-to-machine communications that enable businesses to track inventory, functionality, or efficiency.

Benefits & Risks

Like all technologies, the Internet of Things has benefits and risks. To develop policy approaches to this industry, one must understand both. Below is a summary of the benefits and risks of IoT, both current and potential, highlighted by workshop participants.

Benefits

Most participants agreed that the IoT will offer numerous, and potentially revolutionary, benefits to consumers.[25] One area in which these benefits appear highly promising is health care.[26] For example, insulin pumps and blood-pressure cuffs that connect to a mobile app can enable people to record, track, and monitor their own vital signs, without having to go to a doctor's office. This is especially beneficial for aging patients, for whom connected health devices can provide "treatment options that would allow them to manage their health care at home without the need for long-term hospital stays or transition to a long-term care facility."[27] Patients can also give caregivers, relatives, and doctors access to their health data through these apps, resulting in numerous benefits. As one panelist noted, connected health devices can "improve quality of life and safety by providing a richer source of data to the patient's doctor for diagnosis and treatment[,] . . . improve disease prevention, making the healthcare system more efficient and driving costs down[,] . . . [and] provide an incredible wealth of data, revolutionizing

[25] *See Comment of Future of Privacy Forum*, #484 cmt. #00013 at 4; *Comment of Software & Info. Indus. Ass'n.*, #484 cmt. #00025 at 2.

[26] *See Comment of AT&T Inc.*, #484 cmt. #00004 at 5.

[27] *Comment of Med. Device Privacy Consortium*, #484 cmt. #00022 at 1.

medical research and allowing the medical community to better treat, and ultimately eradicate, diseases."[28]

Recent studies demonstrate meaningful benefits from connected medical devices. One workshop participant said that "one of the most significant benefits that we have from this connected world [is] the ability to . . . draw the patients in and engage them in their own care."[29] Another participant described a clinical trial showing that, when diabetic patients used connected glucose monitors, and their physicians received that data, those physicians were five times more likely to adjust medications, resulting in better disease management and substantial financial savings for patients. He stated that the clinical trial demonstrated that diabetic patients using the connected glucose monitor reduced their average blood sugar levels by two points and that, by comparison, the Food and Drug Administration ("FDA") considers medications that reduce blood sugar by as little as one half point to be successful.[30]

Consumers can benefit from the IoT in many other ways. In the home, for example, smart meters can enable energy providers to analyze consumer energy use and identify issues with home appliances, "even alerting homeowners if their insulation seems inadequate compared to that of their neighbors,"[31] thus empowering consumers to "make better decisions about how they use electricity."[32] Home automation systems can provide consumers with a "single platform that

[28] *Comment of Consumer Elec. Ass'n*, #484 cmt. #00027 at 16.

[29] *See* Remarks of Stan Crosley, Indiana Univ. ("Crosley"), Transcript of Workshop at 199.

[30] *See* Remarks of Anand Iyer, WellDoc Communications, Inc. ("Iyer"), Transcript of Workshop at 188–189.

[31] *Comment of AT&T Inc.*, #484 cmt. #00004 at 4-5.

[32] Remarks of Eric Lightner, Department of Energy ("Lightner"), Transcript of Workshop at 54.

can connect all of the devices within the home, [with] a single app for controlling them."[33] Connected ovens allow consumers to "set [their] temperatures remotely . . . , go from bake to broil . . . , [and] monitor [their] products from various locations inside . . . and outside [their] home[s]."[34] Sensors known as "water bugs" can notify consumers if their basements have flooded,[35] and wine connoisseurs can monitor the temperature in their wine cellars to preserve their finest vintages.[36]

On the road, connected cars will increasingly offer many safety and convenience benefits to consumers. For example, sensors on a car can notify drivers of dangerous road conditions, and software updates can occur wirelessly, obviating the need for consumers to visit the dealership.[37] Connected cars also can "offer real-time vehicle diagnostics to drivers and service facilities; Internet radio; navigation, weather, and traffic information; automatic alerts to first responders when airbags are deployed; and smartphone control of the starter and other aspects of the car."[38] In the future, cars will even drive themselves. Participants discussed the ability of self-driving cars to create safety benefits. For example, rather than having error-prone humans decide which car should go first at a four-way stop sign, self-driving cars will be able to figure out who should

[33] Remarks of Jeff Hagins, SmartThings ("Hagins"), Transcript of Workshop at 64.

[34] Remarks of Michael Beyerle, GE Appliances ("Beyerle"), Transcript of Workshop at 60.

[35] *See* Remarks of Scott Peppet, Univ. of Colorado School of Law ("Peppet"), Transcript of Workshop at 167.

[36] *See* Remarks of Cerf, Transcript of Workshop at 132.

[37] *See* Remarks of Christopher Wolf, Future of Privacy Forum ("Wolf"), Transcript of Workshop at 247-48.

[38] *Comment of Consumer Elec. Ass'n*, #484 cmt. #00027 at 13.

go first according to a standard protocol.[39] They would also allow people with visual impairments to use their own cars as a mode of transportation.[40]

Risks

Despite these important benefits, there was broad agreement among participants that increased connectivity between devices and the Internet may create a number of security and privacy risks.[41]

SECURITY RISKS

According to panelists, IoT devices may present a variety of potential security risks that could be exploited to harm consumers by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating safety risks. Although each of these risks exists with traditional computers and computer networks, they are heightened in the IoT, as explained further below.

First, on IoT devices, as with desktop or laptop computers, a lack of security could enable intruders to access and misuse personal information collected and transmitted to or from the

---

[39] *See* Remarks of Cerf, Transcript of Workshop at 127.

[40] *See id.* at 138.

[41] *See, e.g.*, Remarks of Craig Heffner, Tactical Network Solutions ("Heffner"), Transcript of Workshop at 73-77, 109-10; Remarks of Lee Tien, Electronic Frontier Foundation ("Tien"), Transcript of Workshop at 82-83; Remarks of Hagins, Transcript of Workshop at 92-93, 110; Remarks of Jay Radcliffe, InGuardians, Inc. ("Radcliffe"), Transcript of Workshop at 182-84; Remarks of Iyer, Transcript of Workshop at 223; Remarks of Tadayoshi Kohno, Univ. of Washington ("Kohno"), Transcript of Workshop at 244-47, 263-64; Remarks of David Jacobs, Electronic Privacy Information Center ("Jacobs"), Transcript of Workshop at 296; Remarks of Marc Rogers, Lookout, Inc. ("Rogers"), Transcript of Workshop at 344-45. *See also, e.g.*, HP, INTERNET OF THINGS RESEARCH STUDY 5 (2014), *available at* http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en ("HP Security Research reviewed 10 of the most popular devices in some of the most common IoT niches revealing an alarmingly high average number of vulnerabilities per device. Vulnerabilities ranged from Heartbleed to denial of service to weak passwords to cross-site scripting."); *id.* at 4 (noting that 80 percent of devices tested raised privacy concerns).

device. For example, new smart televisions enable consumers to surf the Internet, make purchases, and share photos, similar to a laptop or desktop computer. [42] Like a computer, any security vulnerabilities in these televisions could put the information stored on or transmitted through the television at risk. If smart televisions or other devices store sensitive financial account information, passwords, and other types of information, unauthorized persons could exploit vulnerabilities to facilitate identity theft or fraud.[43] Thus, as consumers install more smart devices in their homes, they may increase the number of vulnerabilities an intruder could use to compromise personal information.[44]

Second, security vulnerabilities in a particular device may facilitate attacks on the consumer's network to which it is connected, or enable attacks on other systems.[45] For example,

---

[42] *See, e.g.*, Erica Fink & Laurie Segall, *Your TV might be watching you*, CNN MONEY (Aug. 1, 2013), *available at* http://money.cnn.com/2013/08/01/technology/security/tv-hack/index.html ("Today's high-end televisions are almost all equipped with 'smart' PC-like features, including Internet connectivity, apps, microphones and cameras.").

[43] *See* Mario Ballano Barcena *et al.*, *Security Response, How safe is your quantified self?*, SYMANTEC (Version 1.1 – Aug. 11, 2014), *available at* www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/how-safe-is-your-quantified-self.pdf (noting risks relating to IoT including identity theft). According to the most recent statistics from the Bureau of Justice Statistics of the Department of Justice, an estimated 16.6 million Americans – about seven percent of Americans sixteen or older – experienced at least one incident of identity theft in 2012. Losses due to personal identity theft totaled $24.7 billion, billions of dollars more than the losses for all other property crimes *combined*. BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, VICTIMS OF IDENTITY THEFT, 2012 (Dec. 2013)), *available at* http://www.bjs.gov/content/pub/pdf/vit12.pdf. Another study demonstrated that one in four people who received notice of a breach involving their personal information were victims of identity theft, a significantly higher figure than for individuals who did not receive a breach notice. *See* Javelin, 2013 Identity Fraud Report, *available at* https://www.javelinstrategy.com/brochure/276.

[44] *See, e.g.*, Remarks of Marzullo, Transcript of Workshop at 18-19 (discussing ubiquitous or pervasive computing); *id.* at 28-30 (discussing potential security vulnerabilities in devices ranging from pacemakers to automobiles); Remarks of Nguyen, Transcript of Workshop at 35 ("the first thing that really comes to mind are the sensors that are expected to be ubiquitously present and the potential for everything inanimate, whether it be in the home, in the car, or attached to the individual, to measure and transmit data").

[45] *See* Remarks of Heffner, Transcript at 113 ("[I]f I, as someone out on the Internet, can break into a device that is inside your network, I am now inside your network and I can access other things that you do care about . . . . There should never be a device on your network that you shouldn't care about the security of.").

a compromised IoT device could be used to launch a denial of service attack.[46] Denial of service attacks are more effective the more devices the attacker has under his or her control; as IoT devices proliferate, vulnerabilities could enable these attackers to assemble large numbers of devices to use in such attacks.[47] Another possibility is that a connected device could be used to send malicious emails.[48]

Third, unauthorized persons might exploit security vulnerabilities to create risks to physical safety in some cases. One participant described how he was able to hack remotely into two different connected insulin pumps and change their settings so that they no longer delivered medicine.[49] Another participant discussed a set of experiments where an attacker could gain "access to the car's internal computer network without ever physically touching the car."[50] He described how he was able to hack into a car's built-in telematics unit and control the vehicle's engine and braking, although he noted that "the risk to car owners today is incredibly small," in part because "all the automotive manufacturers that I know of are proactively trying to address these things."[51] Although the risks currently may be small, they could be amplified as fully

---

[46] *See, e.g.*, Dick O'Brien, *The Internet of Things: New Threats Emerge in a Connected World*, SYMANTEC (Jan. 21, 2014), *available at* www.symantec.com/connect/blogs/internet-things-new-threats-emerge-connected-world (describing worm attacking IoT devices that connects them to a botnet for use in denial of service attacks).

[47] *Id.*

[48] *See* Paul Thomas, *Despite the News, Your Refrigerator is Not Yet Sending Spam*, SYMANTEC (Jan. 23, 2014), *available at* http://www.symantec.com/connect/blogs/despite-news-your-refrigerator-not-yet-sending-spam (debunking reports that an Internet worm had used compromised IoT devices to send out spam, but adding, "While malware for IoT devices is still in its infancy, IoT devices are susceptible to a wide range of security concerns. So don't be surprised if, in the near future, your refrigerator actually does start sending spam.").

[49] *See* Remarks of Radcliffe, Transcript of Workshop at 182. *See also* Remarks of Tien, Transcript of Workshop at 82-83 ("And obviously one of the big differences between, say, a problem with your phone and a problem with your . . . diabetes pump or your defibrillator is that if it is insecure and it is subject to any kind of malware or attack, it is much more likely there would be very serious physical damage.").

[50] Remarks of Kohno, Transcript of Workshop at 245.

[51] *See id.* at 245-47, 266.

automated cars, and other automated physical objects, become more prevalent. Unauthorized access to Internet-connected cameras or baby monitors also raises potential physical safety concerns.[52] Likewise, unauthorized access to data collected by fitness and other devices that track consumers' location over time could endanger consumers' physical safety. Another possibility is that a thief could remotely access data about energy usage from smart meters to determine whether a homeowner is away from home.

These potential risks are exacerbated by the fact that securing connected IoT devices may be more challenging than securing a home computer, for two main reasons. First, as some panelists noted, companies entering the IoT market may not have experience in dealing with security issues.[53] Second, although some IoT devices are highly sophisticated, many others may be inexpensive and essentially disposable.[54] In those cases, if a vulnerability were discovered after manufacture, it may be difficult or impossible to update the software or apply a patch.[55] And if an update is available, many consumers may never hear about it.[56] Relatedly, many

---

[52] *See* discussion of TRENDnet, *infra* notes 132-34 and accompanying text (FTC settlement alleging that hackers were able to access video streams from TRENDnet cameras). In another notorious incident, a hacker gained access to a video and audio baby monitor. *See* Chris Matyszczyk, *Hacker Shouts at Baby Through Baby Monitor*, CNET (Apr. 29, 2014), *available at* www.cnet.com/news/hacker-shouts-at-baby-through-baby-monitor/. *See also* Kashmir Hill, *'Baby Monitor Hack' Could Happen To 40,000 Other Foscam Users*, FORBES (Aug. 27, 2013), *available at* www.forbes.com/sites/kashmirhill/2013/08/27/baby-monitor-hack-could-happen-to-40000-other-foscam-users/ (recounting a similar incident).

[53] Remarks of Tien, Transcript of Workshop at 71; Remarks of Heffner, Transcript of Workshop at 73-75; Remarks of Hagins, Transcript of Workshop at 92-93.

[54] *See Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 2.

[55] *See, e.g.*, Article 29 Data Protection Working Party, Opinion 8/2014 on Recent Developments on the Internet of Things 9 (Sept. 16, 2014) ("Article 29 Working Group Opinion"), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf ("For example, most of the sensors currently present on the market are not capable of establishing an encrypted link for communications since the computing requirements will have an impact on a device limited by low-powered batteries.").

[56] *Id. See also* Hill, *supra* note 52 (noting that some 40,000 of 46,000 purchasers of connected cameras had not installed a firmware update addressing a security vulnerability).

companies – particularly those developing low-end devices – may lack economic incentives to provide ongoing support or software security updates at all, leaving consumers with unsupported or vulnerable devices shortly after purchase.[57]

PRIVACY RISKS

In addition to risks to security, participants identified privacy risks flowing from the Internet of Things. Some of these risks involve the direct collection of sensitive personal information, such as precise geolocation, financial account numbers, or health information – risks already presented by traditional Internet and mobile commerce. Others arise from the collection of personal information, habits, locations, and physical conditions over time,[58] which may allow an entity that has not directly collected sensitive information to infer it.

The sheer volume of data that even a small number of devices can generate is stunning: one participant indicated that fewer than 10,000 households using the company's IoT home-automation product can "generate 150 million discrete data points a day"[59] or approximately one data point every six seconds for each household.[60]

---

[57] *See, e.g.*, *Bruce Schneier, The Internet of Things Is Wildly Insecure — And Often Unpatchable*, WIRED (Jan. 6, 2014), *available at* http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem ("The problem with this process is that no one entity has any incentive, expertise, or even ability to patch the software once it's shipped. The chip manufacturer is busy shipping the next version of the chip, and the [original device manufacturer] is busy upgrading its product to work with this next chip. Maintaining the older chips and products just isn't a priority.").

[58] *See, e.g.*, Remarks of Tien, Transcript of Workshop at 67; *Comment of Ctr. for Democracy & Tech.*, #484 cmt. #00028 at 4-5.

[59] Remarks of Hagins, Transcript of Workshop at 89.

[60] *Cf. infra* note 73 and accompanying text (discussing inferences possible from smart meter readings taken every two seconds).

Such a massive volume of granular data allows those with access to the data to perform analyses that would not be possible with less rich data sets.[61] According to a participant, "researchers are beginning to show that existing smartphone sensors can be used to infer a user's mood; stress levels; personality type; bipolar disorder; demographics (*e.g.*, gender, marital status, job status, age); smoking habits; overall well-being; progression of Parkinson's disease; sleep patterns; happiness; levels of exercise; and types of physical activity or movement."[62] This participant noted that such inferences could be used to provide beneficial services to consumers, but also could be misused. Relatedly, another participant referred to the IoT as enabling the collection of "sensitive behavior patterns, which could be used in unauthorized ways or by unauthorized individuals."[63] Some panelists cited to general privacy risks associated with these granular information-collection practices, including the concern that the trend towards abundant collection of data creates a "non-targeted dragnet collection from devices in the environment."[64]

Others noted that companies might use this data to make credit, insurance, and employment decisions.[65] For example, customers of some insurance companies currently may opt into programs that enable the insurer to collect data on aspects of their driving habits – such

---

[61] *See* Article 29 Working Group Opinion, *supra* note 55, at 8 ("Full development of IoT capabilities may put a strain on the current possibilities of anonymous use of services and generally limit the possibility of remaining unnoticed.").

[62] Scott R. Peppet, *Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security & Consent*, 93 TEX. L. REV. 85, 115-16 (2014) (citations omitted) ("*Regulating the Internet of Things*"), *available at* http://www.texaslrev.com/wp-content/uploads/Peppet-93-1.pdf. Although we do not include smartphones in our definition of IoT (*see supra* p. 6), many IoT devices contain sensors similar to the sensors in smartphones, and therefore, similar types of inferences may be possible using data from IoT devices.

[63] *Comment of Elec. Privacy Info. Ctr.*, #484 cmt. #00011 at 3.

[64] Remarks of Tien, Transcript of Workshop at 67.

[65] *See* Remarks of Peppet, Transcript of Workshop at 169.

as in one case, the number of "hard brakes," the number of miles driven, and the amount of time spent driving between midnight and 4 a.m. – to help set the insurance rate.[66] Use of data for credit, insurance, and employment decisions could bring benefits – *e.g.*, enabling safer drivers to reduce their rates for car insurance or expanding consumers' access to credit – but such uses could be problematic if they occurred without consumers' knowledge or consent, or without ensuring accuracy of the data.

As a further example, one researcher has hypothesized that although a consumer may today use a fitness tracker solely for wellness-related purposes, the data gathered by the device could be used in the future to price health or life insurance or to infer the user's suitability for credit or employment (*e.g.*, a conscientious exerciser is a good credit risk or will make a good employee).[67] According to one commenter, it would be of particular concern if this type of decision-making were to systematically bias companies against certain groups that do not or cannot engage in the favorable conduct as much as others or lead to discriminatory practices against protected classes.[68]

Participants noted that the Fair Credit Reporting Act ("FCRA")[69] imposes certain limits on the use of consumer data to make determinations about credit, insurance, or employment, or for similar purposes.[70] The FCRA imposes an array of obligations on entities that qualify as

---

[66] *See* Peppet, *Regulating the Internet of Things*, *supra* note 62, at 106-07. *See also*, *e.g.*, Progressive, Snapshot Common Questions, *available at* http://www.progressive.com/auto/snapshot-common-questions/; StateFarm, Drive Safe & Save with In-Drive, *available at* https://www.statefarm.com/insurance/auto/discounts/drive-safe-save/indrive.

[67] *See* Remarks of Peppet, Transcript of Workshop at 167-169.

[68] *See id.* at 93, 123-24.

[69] 15 U.S.C. § 1681 *et seq*.

[70] *See*, *e.g.*, Remarks of Crosley, Transcript of Workshop at 213; Remarks of Peppet, Transcript of Workshop at 213; Peppet, *Regulating the Internet of Things*, *supra* note 62, at 126-127.

consumer reporting agencies, such as employing reasonable procedures to ensure maximum possible accuracy of data and giving consumers access to their information.[71] However, the FCRA excludes most "first parties" that collect consumer information; thus, it would not generally cover IoT device manufacturers that do their own in-house analytics. Nor would the FCRA cover companies that collect data directly from consumers' connected devices and use the data to make in-house credit, insurance, or other eligibility decisions – something that could become increasingly common as the IoT develops. For example, an insurance company may offer consumers the option to submit data from a wearable fitness tracker, in exchange for the prospect of lowering their health insurance premium. The FCRA's provisions, such as those requiring the ability to access the information and correct errors, may not apply in such circumstances.

Yet another privacy risk is that a manufacturer or an intruder could "eavesdrop" remotely, intruding into an otherwise private space. Companies are already examining how IoT data can provide a window into the previously private home.[72] Indeed, by intercepting and analyzing unencrypted data transmitted from a smart meter device, researchers in Germany were

---

[71] *See* 15 U.S.C. §§1681e, 1681j.

[72] *See, e.g.*, Louise Downing, *WPP Unit, Onzo Study Harvesting Smart-Meter Data*, BLOOMBERG (May 12, 2014), *available at* http://origin-www.bloomberg.com/apps/news?pid=conewsstory&tkr=WPP:LN&sid=aPY7EUU9oD6g (reporting that the "world's biggest advertising agency" and a software company are collaborating to explore uses of smart meter data and quoting a CEO who noted, "Consumers are leaving a digital footprint that opens the door to their online habits and to their shopping habits and their location, and the last thing that is understood is the home, because at the moment, when you shut the door, that is it."). *See also Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 2-3 ("to the extent that a powerful commercial entity controls an IoT networking platform within a home or business, that positions them to collect, analyze, and act upon copious amounts of data from within traditionally private spaces.").

able to determine what television show an individual was watching.[73] Security vulnerabilities in camera-equipped devices have also raised the specter of spying in the home.[74]

Finally, some participants pointed out that perceived risks to privacy and security, even if not realized, could undermine the consumer confidence necessary for the technologies to meet their full potential and may result in less widespread adoption.[75] As one participant stated, "promoting privacy and data protection principles remains paramount to ensure societal acceptance of IoT services."[76]

[73] *See* Dario Carluccio & Stephan Brinkhaus, Presentation: "Smart Hacking for Privacy," 28th Chaos Communication Congress, Berlin, December 2011, *available at* https://www.youtube.com/watch?v=YYe4SwQn2GE&feature=youtu.be. Moreover, "the two-second reporting interval provides so much data that [the researchers] were able to accurately chart power usage spikes and lulls indicative of times a homeowner would be home, asleep or away." *Id.* (In most smart meter implementations, data is reported at much longer intervals, usually fifteen minutes.) In addition to the privacy concerns, as noted above, the researchers discovered that the encryption was not implemented properly and that they could alter the energy consumption data reported by the meter. *Id.*

[74] *See, e.g.*, Fink & Segall, *supra* note 42 (describing a security vulnerability in Samsung smart TVs, since patched, that "enabled hackers to remotely turn on the TVs' built-in cameras without leaving any trace of it on the screen").

[75] *See, e.g.*, *Comment of Consumer Elec. Ass'n*, #484 cmt. #00027 at 17-18; *Comment of CTIA – The Wireless Ass'n*, #510 cmt. #00014 at 2; *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 5.

[76] *Comment of GS1 US*, #484 cmt. #00030 at 4.

Application of Traditional Privacy Principles

Summary of Workshop Discussions

Participants debated how the long-standing Fair Information Practice Principles ("FIPPs") of notice, choice, access, accuracy, data minimization, security, and accountability should apply to the IoT space. While some participants continued to support the application of all of the FIPPs,[77] others argued that data minimization, notice, and choice are less suitable for protecting consumer privacy in the IoT.[78]

The FIPPs were first articulated in 1973 in a report by what was then the U.S. Department of Health, Education and Welfare.[79] Subsequently, in 1980, the Organization for Economic Cooperation and Development ("OECD") adopted a set of privacy guidelines, which embodied the FIPPs.[80] Over time, the FIPPs have formed the basis for a variety of both government and private sector initiatives on privacy. For example, both the European Union

[77] *See, e.g.*, Remarks of Michelle Chibba, Office of the Information and Privacy Commissioner, Ontario, Canada ("Chibba"), Transcript of Workshop at 329; Remarks of Jacobs, Transcript of Workshop at 328-329; *Comment of AAA*, #510 cmt. #00012 at 2; *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 3.

[78] *See, e.g.*, *Comment of GS1 US*, #484 cmt. #00030 at 5; *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. # 00021 at 2; *Comment of Info. Tech. Indus. Council*, #510 cmt. #00008 at 3.

[79] *See* FTC, PRIVACY ONLINE: A REPORT TO CONGRESS 48 n.27 (1998), *available at* http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

[80] *See* OECD, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), *available at* http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. (In 2013, the OECD updated its guidelines to address risk management, interoperability, and other issues. The update is available at http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf). *See also* FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS 3-4, 43 n.25 (2000).

Directive on the protection of personal data[81] and the Health Insurance Portability and Accountability Act ("HIPAA")[82] are based, in large part, on the FIPPs. In addition, many self-regulatory guidelines include the principles of notice, choice, access, and security.[83] The Obama Administration's Consumer Privacy Bill of Rights also includes these principles,[84] as does the privacy framework set forth in the Commission's 2012 Privacy Report.[85]

Workshop discussion focused on four FIPPs in particular – data security, data minimization, notice, and choice. As to data security, there was widespread agreement on the need for companies manufacturing IoT devices to incorporate reasonable security into these devices. As one participant stated, "Inadequate security presents the greatest risk of actual consumer harm in the Internet of Things."[86] Accordingly, as another participant noted,

---

[81] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31, *available at* http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

[82] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

[83] *See, e.g.*, NETWORK ADVER. INITIATIVE, NAI CODE OF CONDUCT 2013, *available at* http://www.networkadvertising.org/2013_Principles.pdf; INTERNET ADVER. BUREAU, INTERACTIVE ADVERTISING PRIVACY PRINCIPLES (Feb. 24, 2008), *available at* http://www.iab.net/guidelines/508676/1464.

[84] THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[85] FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS vii-viii (2012) ("Privacy Report"), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf. Commissioners Ohlhausen and Wright were not members of the Commission at that time and thus did not offer any opinion on that matter.

[86] *Comment of Future of Privacy Forum*, #510 cmt. #00013 at 9 (and listing types of security measures that are already being implemented to secure the IoT).

"[s]ecurity must be built into devices and networks to prevent harm and build consumer trust in the IoT." [87]

Participants were more divided about the continuing applicability of the principles of data minimization, notice, and choice to the IoT.[88] With respect to data minimization – which refers to the concept that companies should limit the data they collect and retain, and dispose of it once they no longer need it – one participant expressed concerns that requiring fledgling companies to predict what data they should minimize would "chok[e] off potential benefits and innovation."[89] A second participant cautioned that "[r]estricting data collection with rules like data minimization could severely limit the potential opportunities of the Internet of Things" based on beneficial uses that could be found for previously-collected data that were not contemplated at the time of collection.[90] Still another participant noted that "[d]ata-driven innovation, in many ways, challenges many interpretations of data minimization where data purpose specification and use limitation are overly rigid or prescriptive."[91]

With respect to notice and choice, some participants expressed concern about its feasibility, given the ubiquity of IoT devices and the persistent and pervasive nature of the

---

[87] *Comment of Infineon Tech. N. Am. Corp.*, #510 cmt. #00009 at 2; *see also* Remarks of Rogers, Transcript of Workshop at 312 ("There are some pretty good examples out there of what happens to companies when security becomes an afterthought and the cost that companies can incur in trying to fight the damage, the cost to brand reputation, the loss of customer confidence. And there are also some great examples of companies, even in the Internet of Things, as new as it is, companies that have gotten it right and they've done well. And they've gone on to push out products where there have been no issues.").

[88] *See, e.g.*, *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. # 00021 at 2; *Comment of Info. Tech. Indus. Council*, #510 cmt. #00008 at 3-4.

[89] Remarks of Dan Caprio, McKenna, Long & Aldridge, LLP ("Caprio"), Transcript of Workshop at 339.

[90] *Comment of Ctr. for Data Innovation*, #510 cmt. #00002 at 3.

[91] *Comment of Software & Info. Indus. Ass'n*, #484 cmt. #00025 at 6–7; *see also Comment of Future of Privacy Forum*, #510 cmt. #00013 at 5 (purpose specification and data minimization as applied to the IoT "risks unduly limiting the development of new services and the discoveries that may follow from valuable research").

information collection that they make possible. As one participant observed, when "a bunch of different sensors on a bunch of different devices, on your home, your car, your body . . . are measuring all sorts of things," it would be burdensome both for the company to provide notice and choice, and for the consumer to exercise such choice every time information was reported.[92] Another participant talked about the risk that, if patients have "to consent to everything" for a health monitoring app, "patients will throw the bloody thing away."[93] Yet another participant noted that any requirement to obtain consent could be "a barrier to socially beneficial uses of information."[94]

A related concern is that many IoT devices – such as home appliances or medical devices – have no screen or other interface to communicate with the consumer, thereby making notice on the device itself difficult, if not impossible.[95] For those devices that do have screens, the screens may be smaller than even the screens on mobile devices, where providing notice is already a challenge.[96] Finally, even if a device has screens, IoT sensors may collect data at times when the consumer may not be able to read a notice (for example, while driving).[97]

---

[92] Remarks of Peppet, Transcript of Workshop at 215–16.

[93] Remarks of Iyer, Transcript of Workshop at 230.

[94] *Comment of Software & Info. Indus. Ass'n*, #484 cmt. #00025 at 8.

[95] *See, e.g., Comment of Ctr. for Data Innovation*, #510 cmt. #00002 at 2; *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 2 and 6; *Comment of Transatl. Computing Continuum Policy Alliance*, #510 cmt. #00017 at 2.

[96] *See* FTC STAFF REPORT, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 10–11 (2013) ("Mobile Disclosures Report"), *available at* http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

[97] In addition, some participants also suggested that notice and choice is not workable for IoT products and services that are not consumer-facing – *e.g.*, a sensor network to monitor electricity use in hotels. *See, e.g.*, *Comment of GS1 US*, #484 cmt. #00030 at 5 (noting that "[i]t is difficult to anticipate how the existing mechanisms of notice and choice, both being sound principles for privacy protection, would apply to sensors. . . . [H]ow would one provide adequate notice for every embedded sensor network? How would consent be obtained?"); *Comment of Future of*

Despite these challenges, participants discussed how companies can provide data minimization, notice, and choice within the IoT. One participant suggested that, as part of a data minimization exercise, companies should ask themselves a series of questions, such as whether they need a particular piece of data or whether the data can be deidentified.[98] Another participant gave a specific example of how data could be minimized in the context of connected cars. This participant noted that the recording device on such cars could "automatically delete old data after a certain amount of time, or prevent individual data from being automatically synched with a central database."[99]

As to notice and choice, one auto industry participant noted that his company provides consumers with opt-in choices at the time of purchase in "[p]lain language and multiple choices of levels."[100] Another discussed a "consumer profile management portal[]" approach that would include privacy settings menus that consumers can configure and revisit,[101] possibly on a separate device such as a smartphone or a webportal. In addition to the types of specific settings and choices, another participant suggested that devices and their associated platforms could enable consumers to aggregate choices into "packets."[102] Finally, one participant noted that

---

Privacy Forum, #510 cmt. #00013, Appendix A at 4. As noted above, this report addresses privacy and security practices for consumer-facing products.

[98] Remarks of Chibba, Transcript of Workshop at 300-01.

[99] Comment of EPIC, #484 cmt. #00011 at 17-18.

[100] Remarks of Kenneth Wayne Powell, Toyota Technical Center ("Powell"), Transcript of Workshop at 278.

[101] *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 6.

[102] Remarks of Joseph Lorenzo Hall, Center for Democracy & Technology ("Hall"), Transcript of Workshop at 216.

companies could consider an approach that applies learning from consumer behavior on IoT devices, in order to personalize privacy choices.[103]

Some participants advocated for an increased focus on certain types of use restrictions to protect consumer data.[104] With this approach, legislators, regulators, self-regulatory bodies, or individual companies would set "permissible" and "impermissible" uses of certain consumer data. One commenter characterized this approach as "shifting responsibility away from data subjects toward data users, and increasing the emphasis on responsible data stewardship and accountability."[105]

Participants offered a variety of approaches to adding use-based data protections. One participant proposed that companies "tag" data with its appropriate uses so that automated processes could identify and flag inappropriate uses.[106] Other participants noted that policymakers could constrain certain uses of IoT data that do not comport with consumer expectations and present the most risk of harm, either through law[107] or through voluntary

[103] Remarks of Nguyen, Transcript of Workshop at 48.

[104] *See* Remarks of Peppet, Transcript of Workshop at 210-211 (advocating "drawing some lines around acceptable use" through legislation or regulation in addition to notice and choice); *see also* Remarks of Crosley at 213 (supporting "the appropriate use of the context"); Remarks of Hall at 214 (expressing support for "[u]se restrictions, as long as they have teeth. That's why I think vanilla self-regulatory efforts are probably not the answer. You need to have something that is enforced by an independent body").

[105] Comment of Software & Information Industry Association, #484 cmt #00025 at 8.

[106] *Comment of Future of Privacy Forum*, #510 cmt. #00013 at 10–11 (citing 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). We note that such an approach would require coordination and potential associated costs.

[107] *See* Peppet, *Regulating the Internet of Things*, *supra* note 62, at 149 (proposing regulatory constraints).

self-regulatory efforts[108] or seal programs.[109] For example, as one participant has pointed out, some state laws restrict access by auto insurance companies and other entities to consumers' driving data recorded by an EDR.[110]

Post-Workshop Developments

Since the November 2013 workshop, the IoT marketplace has continued to develop at a remarkable pace. For example, in June 2014, Apple announced "HealthKit," a platform that "functions as a dashboard for a number of critical metrics as well as a hub for select third-party fitness products,"[111] as a way to help protect health information that some connected devices may collect. Similarly, in October 2014, Microsoft announced Microsoft Health, a "cloud-based service that … provid[es] actionable insights based on data gathered from the fitness devices and apps" and which will work in conjunction with Microsoft's HealthVault, which for a decade has offered "a trusted place to store health information and share it with medical professionals on a security-enhanced platform."[112] And last November, Intel announced a "new platform …

[108] *See, e.g.*, *Comment of Consumer Elec. Ass'n*, #484 cmt. #00027 at 7; *Comment of Direct Mktg. Ass'n*, #484 cmt. #00010 at 2; *Comment of CTIA – The Wireless Ass'n*, # 510 cmt. #00014 at 4; *Comment of U.S. Chamber of Commerce*, #510 cmt. #00011 at 3.

[109] *See, e.g.*¸*Comment of AT&T Inc.*, #484 cmt. #00004 at 9–10; *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 13.

[110] Peppet, *Regulating the Internet of Things*, *supra* note 62, at 153-54.

[111] Rachel King, *Apple takes app-based approach to health tech with HealthKit*, ZDNet (June 2, 2014), *available at* http://www.zdnet.com/article/apple-takes-app-based-approach-to-health-tech-with-healthkit/.

[112] Microsoft Health, http://www.microsoft.com/Microsoft-Health/en-us (last visited Jan. 9, 2015).

designed to make it easier for developers to connect devices securely, bring device data to the cloud, and make sense of that data with analytics."[113]

Policymakers have also tried to keep pace with these developments in the IoT. For example, in May 2014, the White House released a Big Data report ("White House Big Data Report"), and the President's Council of Advisors on Science and Technology released a companion report ("PCAST Report"). Both reports weigh in on the debate between the application of data minimization, notice, and choice versus use limitations. The White House Big Data Report opined that "the notice and consent framework threatens to be overcome" in certain instances, "such as the collection of ambient data by our household appliances."[114] The White House Big Data Report concluded that,

> Putting greater emphasis on a responsible use framework has many potential advantages. It shifts the responsibility from the individual, who is not well equipped to understand or contest consent notices as they are currently structured in the marketplace, to the entities that collect, maintain, and use data. Focusing on responsible use also holds data collectors and users accountable for how they manage the data and any harms it causes, rather than narrowly defining their responsibility to whether they properly obtained consent at the time of collection.[115]

Attention to the impact of the IoT spans the globe. In September 2014, Europe's Article 29 Working Group – composed of data protection authorities of EU member countries – issued

---

[113] Aaron Tilley, Intel Releases New Platform To Kickstart Development In The Internet Of Things, FORBES (Dec. 9, 2014), *available at* http://www.forbes.com/sites/aarontilley/2014/12/09/intel-releases-new-platform-to-kickstart-development-in-the-internet-of-things/.

[114] Executive Office of the President, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (May 2014) ("White House Big Data Report") at 56, *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf. *See also* President's Council of Advisors on Science and Technology, REPORT TO THE PRESIDENT: BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 38 (May 2014), *available at* http://www.whitehouse.gov/administration/eop/ostp/pcast.

[115] *White House Big Data Report* at 56.

an Opinion on Recent Developments on the Internet of Things.[116] In the opinion, the Working Group emphasized the importance of user choice, noting that "users must remain in complete control of their personal data throughout the product lifecycle, and when organisations rely on consent as a basis for processing, the consent should be fully informed, freely given and specific."

In addition to policy work by government agencies, standards organizations related to the Internet of Things continue to proliferate. One such area for standard-setting is data security. For example, in August 2014, oneM2M, a global standards body, released a proposed security standard for IoT devices. The standard addresses issues such as authentication, identity management, and access control.[117]

Commission Staff's Views and Recommendations for Best Practices

This section sets forth the Commission staff's views on the issues of data security, data minimization, and notice and choice with respect to the IoT and provides recommendations for best practices for companies.

DATA SECURITY

As noted, there appeared to be widespread agreement that companies developing IoT products should implement reasonable security. Participants also discussed a number of specific security best practices. The Commission staff encourages companies to consider adopting these

[116] Article 29 Working Group Opinion, *supra* note 55.

[117] *See* oneM2M, *Technical Specification*, *oneM2M Security Solutions* at 15-16, *available at* http://www.onem2m.org/images/files/deliverables/TS-0003-Security_Solutions-V-2014-08.pdf.

practices. Of course, what constitutes reasonable security for a given device will depend on a number of factors, including the amount and sensitivity of data collected, the sensitivity of the device's functionality, and the costs of remedying the security vulnerabilities. Nonetheless, the specific security best practices companies should consider include the following:

First, companies should implement "security by design" by building security into their devices at the outset, rather than as an afterthought.[118] One participant stated that security should be designed into every IoT product, at every stage of development, including "early on in the design cycle of a technology."[119] In addition, a company should do a privacy or security risk assessment, consciously considering the risks presented by the collection and retention of consumer information.[120] As part of this process, companies should incorporate the use of smart defaults, such as requiring consumers to change default passwords – if they use default passwords at all – during the set-up process.[121] Companies also should consider how to minimize the data they collect and retain, as discussed further below. Finally, companies should test their security measures before launching their products. As one participant pointed out, such testing should occur because companies – and service providers they might use to help develop their

[118] *Comment of ARM and AMD*, #510 cmt. #00018 at 2; *see also* Remarks of Hagins, Transcript of Workshop at 111; Remarks of Jacobs, Transcript of Workshop at 296; Remarks of Caprio, Transcript of Workshop at 298.

[119] Remarks of Kohno, Transcript of Workshop at 281.

[120] Remarks of Chibba, Transcript of Workshop at 301; *see also* Remarks of Rogers, Transcript of Workshop at 343.

[121] *See generally* Remarks of Rogers, Transcript of Workshop at 344 ("Default passwords are something that should never pass through into production space. It's an easy thing to pick up with a very basic assessment, yet we are constantly seeing these come through because these companies aren't often doing this kind of assessment − so they see it as a hindrance, an extra step. Or they claim the consumer should be responsible for setting the security, once it lands on the consumer's desk which, at the end of the day, the consumers aren't capable of setting that level of security, nor should they have to.").

products – may simply forget to close "backdoors" in their products through which intruders could access personal information or gain control of the device.[122]

This last point was illustrated by the Commission's recent actions against the operators of the Credit Karma and Fandango mobile apps. In these cases, the companies overrode the settings provided by the Android and iOS operating systems, so that SSL encryption was not properly implemented. As a result, the Commission alleged, hackers could decrypt the sensitive consumer financial information being transmitted by the apps. The orders in both cases include provisions requiring the companies to implement reasonable security.[123]

Second, companies must ensure that their personnel practices promote good security. As part of their personnel practices, companies should ensure that product security is addressed at the appropriate level of responsibility within the organization. One participant suggested that "if someone at an executive level has responsibility for security, it tends to drive hiring and processes and mechanisms throughout the entire organization that will improve security."[124] Companies should also train their employees about good security practices, recognizing that technological expertise does not necessarily equate to security expertise. Indeed, one participant stated that being able to write software code "doesn't mean…understand[ing] anything whatsoever about the security of an embedded device."[125]

---

[122] *See generally* Remarks of Heffner, Transcript of Workshop at 73-74.

[123] Credit Karma, Inc., File No. 132-3091 (Mar. 28, 2014) (consent), *available at* http://www.ftc.gov/enforcement/cases-proceedings/132-3091/credit-karma-inc; Fandango, LLC, File No. 132-3089 (Mar. 28, 2014) (consent), *available at* http://www.ftc.gov/enforcement/cases-proceedings/132-3089/fandango-llc. *See also* HTC America, Inc., No. C-4406 (July 2, 2013) (consent) (alleging that HTC, among other things, failed to conduct assessments, audits, reviews, or tests to identify potential security vulnerabilities in its mobile devices), *available at* http://www.ftc.gov/enforcement/cases-proceedings/122-3049/htc-america-inc-matter.

[124] Remarks of Hagins, Transcript of Workshop at 110.

[125] *Id.* at 92.

Third, companies must work to ensure that they retain service providers that are capable of maintaining reasonable security, and provide reasonable oversight to ensure that those service providers do so. Failure to do so could result in an FTC law enforcement action. For example, in the Commission's recent settlement with GMR Transcription Services, the Commission alleged that a medical and legal transcription company outsourced transcription services to independent typists in India without adequately checking to make sure they could implement reasonable security measures. According to the Commission's complaint, among other things, the service provider stored transcribed notes in clear text on an unsecured server. As a result, U.S. consumers found their doctors' notes of their physical examinations freely available through Internet searches. This case illustrates the strong need for appropriate service provider oversight.

Fourth, for systems with significant risk, companies should implement a defense-in-depth approach, where security measures are considered at several levels. For example, participants raised concerns about relying on the security of consumers' own networks, such as passwords for their Wi-Fi routers, alone to protect the information on connected devices.[126] They noted that companies must take "additional steps to encrypt [the information] or otherwise secure it."[127] FTC staff shares these concerns and encourages companies to take additional steps to secure information passed over consumers' home networks. Indeed, encryption for sensitive information, such as that relating to health, is particularly important in this regard.[128] Regardless of the specific technology, companies should reasonably secure data in transit and in storage.

[126] *Id.* at 102.

[127] Remarks of Heffner, Transcript of Workshop at 102-03.

[128] Remarks of Hall, Transcript of Workshop at 178-79.

Fifth, panelists noted that companies should consider implementing reasonable access control measures to limit the ability of an unauthorized person to access a consumer's device, data, or even the consumer's network.[129] In the IoT ecosystem, strong authentication could be used to permit or restrict IoT devices from interacting with other devices or systems. The privileges associated with the validated identity determine the permissible interactions between the IoT devices and could prevent unauthorized access and interactions.[130] In implementing these protections, companies should ensure that they do not unduly impede the usability of the device. As noted above, the proposed oneM2M security standard includes many of the recommendations discussed above.[131] Such efforts are important to the success of IoT.

Finally, companies should continue to monitor products throughout the life cycle and, to the extent feasible, patch known vulnerabilities. Many IoT devices have a limited life cycle, resulting in a risk that consumers will be left with out-of-date IoT devices that are vulnerable to critical, publicly known security or privacy bugs. Companies may reasonably decide to limit the time during which they provide security updates and software patches, but it is important that companies weigh these decisions carefully. Companies should also be forthright in their representations about providing ongoing security updates and software patches. Disclosing the length of time companies plan to support and release software updates for a given product line will help consumers better understand the safe 'expiration dates' for their commodity Internet-

---

[129] *See, e.g.*, BRETT C. TJADEN, FUNDAMENTALS OF SECURE COMPUTER SYSTEMS 5 (2004). *See also* HP, INTERNET OF THINGS RESEARCH STUDY, *supra* note 41, at 4-5 (noting that approximately 60% of IoT devices examined had weak credentials).

[130] There may be other appropriate measures, as the security measures that a company should implement vary, depending on the risks presented by unauthorized access to the device, and the sensitivity of any information collected.

[131] oneM2M Candidate Release August 2014, *available at* http://www.onem2m.org/technical/candidate-release-august-2014 (last visited Dec. 19, 2014).

connected devices. In addition, companies that do provide ongoing support should also notify consumers of security risks and updates.

Several of these principles are illustrated by the Commission's first case involving an Internet-connected device. TRENDnet[132] marketed its Internet-connected cameras for purposes ranging from home security to baby monitoring, claiming that they were "secure." In its complaint, the Commission alleged, among other things, that the company transmitted user login credentials in clear text over the Internet, stored login credentials in clear text on users' mobile devices, and failed to test consumers' privacy settings to ensure that video feeds marked as "private" would in fact be private.[133] As a result of these alleged failures, hackers were able to access live feeds from consumers' security cameras and conduct "unauthorized surveillance of infants sleeping in their cribs, young children playing, and adults engaging in typical daily activities."[134] This case demonstrates the importance of practicing security-by-design.

[132] Press Release, FTC, Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy (Sept. 4, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles.

[133] Complaint of FTC, TRENDnet, Inc., No. C-4426 (Feb. 7, 2014) (consent), *available at* http://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

[134] *Id*. at 5.

Of course, the IoT encompasses a wide variety of products and services, and, as noted, the specific security measures that a company needs to implement will depend on a number of factors.[135] Devices that collect sensitive information, present physical security or safety risks (such as door locks, ovens, or insulin pumps), or connect to other devices or networks in a manner that would enable intruders to access those devices or networks should be more robustly secured than, for example, devices that simply monitor room temperatures, miles run, or calories ingested.

DATA MINIMIZATION

Commission staff agrees with workshop participants who stated that the data minimization principle remains relevant and important to the IoT.[136] While staff recognizes that companies need flexibility to innovate around new uses of data, staff believes that these interests can and should be balanced with the interests in limiting the privacy and data security risks to consumers.[137] Accordingly, companies should examine their data practices and business needs

[135] *See, e.g.*, FTC, Commission Statement Marking the FTC's 50th Data Security Settlement (Jan. 31, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf:

> The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities. Through its settlements, testimony, and public statements, the Commission has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.

[136] *See, e.g.*, Remarks of Tien, Transcript of Workshop at 107–08; *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 6–7.

[137] *See, e.g.*, *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 3; Remarks of Chibba, Transcript of Workshop at 329–30.

and develop policies and practices that impose reasonable limits on the collection and retention of consumer data.[138]

Data minimization is a long-standing principle of privacy protection and has been included in several policy initiatives, including the 1980 OECD Privacy Guidelines, the 2002 Asia-Pacific Economic Cooperation ("APEC") Privacy Principles, and the 2012 White House Consumer Privacy Bill of Rights.[139] Some observers have debated how data minimization would apply to new technologies.[140] In the IoT ecosystem, data minimization is challenging, but it remains important.[141] Indeed, data minimization can help guard against two privacy-related risks. First, collecting and retaining large amounts of data increases the potential harms associated with a data breach, both with respect to data stored on the device itself as well as in the cloud. Larger data stores present a more attractive target for data thieves, both outside and inside a company –

---

[138] Privacy Report, *supra* note 85, at 26–27; *see also* Mobile Disclosures Report, *supra* note 96, at 1 n.2; FTC, Data Brokers: A Call for Transparency and Accountability 55 (2014) ("Data Broker Report"), *available at* http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[139] *See* Privacy Report, *supra* note 85, at 26–27; OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, at ¶ 7 (2013), *available at* http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (same); Dept. of Homeland Security, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security § 5 (Dec. 29, 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf (stating a Data Minimization principle: "DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s)."); Exec. Office of the President, National Strategy for Trusted Identities in Cyberspace 45 (Apr. 2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf (stating a Data Minimization principle: "Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).").

[140] *See* White House Big Data Report, *supra* note 114, at 54 (Because "the logic of collecting as much data as possible is strong … focusing on controlling the collection and retention of personal data, while important, may no longer be sufficient to protect personal privacy."); PCAST Report at x-xi ("[A] policy focus on limiting data collection will not be a broadly applicable or scalable strategy – nor one likely to achieve the right balance between beneficial results and unintended negative consequences (such as inhibiting economic growth).").

[141] *See, e.g.*, Remarks of Tien, Transcript of Workshop at 107–08; *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 6–7. *See also* Article 29 Working Group Opinion, *supra* note 55, at 16–17.

and increases the potential harm from such an event.[142] Thieves cannot steal data that has been deleted after serving its purpose; nor can thieves steal data that was not collected in the first place. Indeed, in several of its data security cases, the Commission has alleged that companies could have mitigated the harm associated with a data breach by disposing of customer information they no longer had a business need to keep.[143]

Second, if a company collects and 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. For example, in 2010, Commission staff sent a letter to the founders of XY magazine, a magazine for gay youth, regarding their negotiations to sell in bankruptcy customer information dating back to as early as 1996. The staff noted that, because the magazine had ceased to exist for a period of three years, the subscribers were likely to have become adults and moved on, and because continued use of their information would have been contrary to their reasonable expectations, XY should delete the personal information.[144] In this case, the risk associated with continued storage and use of the subscribers' personal information contrary to their reasonable expectations would not have existed if the company had engaged in reasonable data minimization practices.

Although these examples are not IoT-specific, they demonstrate the type of risk created by the expansive collection and retention of data. To minimize these risks, companies should

---

[142] Remarks of Chibba, Transcript of Workshop at 340; Privacy Report, *supra* note 85, at 27–29.

[143] *See CardSystems Solutions, Inc.*, No. C-4168, 2006 WL 2709787 (F.T.C. Sept. 5, 2006) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/052-3148/cardsystems-solutions-inc-solidus-networks-inc-dba-pay-touch; *DSW, Inc.*, No. C-4157, 2006 WL 752215 (F.T.C. Mar. 7, 2006) (consent order); *BJ's Wholesale Club, Inc.*, 140 F.T.C. 465 (2005) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/042-3160/bjs-wholesale-club-inc-matter. Commissioner Ohlhausen was not a commissioner at the time of these cases and therefore did not participate in them.

[144] Letter from David C. Vladeck, Dir., FTC Bureau of Consumer Prot., to Peter Larson and Martin E. Shmagin (July 1, 2010), *available at* http://www.ftc.gov/enforcement/cases-proceedings/closing-letters/letter-xy-magazine-xycom-regarding-use-sale-or.

examine their data practices and business needs and develop policies and practices that impose reasonable limits on the collection and retention of consumer data.[145] Such an exercise is integral to a privacy-by-design approach and helps ensure that the company has given thought to its data collection practices on the front end by asking questions such as what types of data it is collecting, to what end, and how long it should be stored.[146] The process of mindfully considering data collection and retention policies and engaging in a data minimization exercise could also serve an education function for companies, while at the same time, protecting consumer privacy.[147]

As an example of how data minimization might work in practice, suppose a wearable device, such as a patch, can assess a consumer's skin condition. The device does not need to collect precise geolocation information in order to work; however, the device manufacturer believes that such information might be useful for a future product feature that would enable users to find treatment options in their area. As part of a data minimization exercise, the company should consider whether it should wait to collect geolocation until after it begins to offer the new product feature, at which time it could disclose the new collection and seek consent. The company should also consider whether it could offer the same feature while collecting less information, such as by collecting zip code rather than precise geolocation. If the company does decide it needs the precise geolocation information, it should provide a prominent disclosure about its collection and use of this information, and obtain consumers' affirmative

[145] *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. #00021 at 4.

[146] *Id. See also* Remarks of Chibba, Transcript of Workshop at 330.

[147] *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. #00021 at 4.

express consent. Finally, it should establish reasonable retention limits for the data it does collect.

To the extent that companies decide they need to collect and maintain data to satisfy a business purpose, they should also consider whether they can do so while maintaining data in de-identified form. This may be a viable option in some contexts and helps minimize the individualized data companies have about consumers, and thus any potential consumer harm, while promoting beneficial societal uses of the information. For example, one university hospital offers a website and an associated smart phone app that collect information from consumers, including geolocation information, to enable users to find and report flu activity in their area.[148] The hospital can maintain and post information in anonymous and aggregate form, which can benefit public health authorities and the public, while at the same time maintaining consumer privacy.

A key to effective de-identification is to ensure that the data cannot be reasonably re-identified. For example, U.S. Department of Health and Human Service regulations[149] require entities covered by HIPAA to either remove certain identifiers, such as date of birth and five-digit zip code, from protected health information[150] or have an expert determine that the risk of re-identification is "very small."[151] As one participant discussed,[152] in 2009, a group of experts attempted to re-identify approximately 15,000 patient records that had been de-identified under

[148] *See* Flu Near You, *available at* https://flunearyou.org/.

[149] 45 C.F.R. §§ 164.514(a)-(c).

[150] 45 C.F.R. § 165.514(b)(2).

[151] 45 C.F.R. § 165.514(b)(1).

[152] *Comment of Future of Privacy Forum*, #510 cmt. #00013, Appendix A at 8.

the HIPAA standard. They used commercial data sources to re-identify the data and were able to identify only 0.013% of the individuals.[153] While deidentification can be challenging in several contexts,[154] appropriately de-identified data sets that are kept securely and accompanied by strong accountability mechanisms, can reduce many privacy risks.

Of course, as technology improves, there is always a possibility that purportedly de-identified data could be re-identified.[155] This is why it is also important for companies to have accountability mechanisms in place. When a company states that it maintains de-identified or anonymous data, the Commission has stated that companies should (1) take reasonable steps to de-identify the data, including by keeping up with technological developments; (2) publicly commit not to re-identify the data; and (3) have enforceable contracts in place with any third parties with whom they share the data, requiring the third parties to commit not to re-identify the data.[156] This approach ensures that if the data is not reasonably de-identified and then is re-identified in the future, regulators can hold the company responsible.

With these recommendations on data minimization, Commission staff is mindful of the need to balance future, beneficial uses of data with privacy protection. For this reason, staff's recommendation is a flexible one that gives companies many options: they can decide not to

---

[153] *Id.*

[154] Technical experts continue to evaluate the effectiveness of deidentification for different types of data, and some urge caution in interpreting claims about the effectiveness of specific technical means of deidentification. *See, e.g.*, Arvind Narayanan and Edward Felten, No Silver Bullet: De-Identification Still Doesn't Work (July 9, 2014), *available at* http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf.

[155] *See, e.g.*, Ann Cavoukian and Khaled El Emam, De-identification Protocols: Essential for Protecting Privacy (June 25, 2014), *available at* http://www.privacybydesign.ca/content/uploads/2014/06/pbd-de-identifcation_essential.pdf; *Comment of Ctr. for Democracy & Tech*, #510 cmt. #00016 at 8; Privacy Report, *supra* note 85, at 21.

[156] *See* Privacy Report, *supra* note 85, at 21; *see also Comment of Future of Privacy Forum*, #510 cmt. #00013, Appendix A at 7.

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 de-identify the data they collect. If a company determines that none of these options work, it can seek consumers' consent for collecting additional, unexpected data. In addition, in considering reasonable collection and retention limits, it is appropriate to consider the sensitivity of the data at issue: the more sensitive the data, the more harmful it could be if the data fell into the wrong hands or were used for purposes the consumer would not expect. Through this approach, a company can minimize its data collection, consistent with its business goals.[157] As one participant noted, "[p]rotecting privacy and enabling innovation are not mutually exclusive and must consider principles of accountability and privacy by design."[158]

NOTICE AND CHOICE

While the traditional methods of providing consumers with disclosures and choices may need to be modified as new business models continue to emerge, staff believes that providing notice and choice remains important, as potential privacy and security risks may be heightened due to the pervasiveness of data collection inherent in the IoT. Notice and choice is particularly important when sensitive data is collected.[159]

---

[157] *See, e.g.*, *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 10 (describing its Smart Grid privacy seal).

[158] *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. #00021 at 3. *See also* Remarks of Chibba, Transcript of Workshop at 330.

[159] *See, e.g.*, *Comment of Future of Privacy Forum*, #510 cmt. #00013 at 6 ("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."); *Comment of Ctr. for Digital Democracy*, #484 cmt. #00006 at 3 ("[T]he combined impact of the mobile marketing and real-time data revolution and the Internet of Things places consumer privacy at greater risk than ever before.").

Moreover, staff believes that providing consumers with the ability to make informed choices remains practicable in the IoT. This does not mean that every data collection requires choice. The Commission has recognized that providing choices for every instance of data collection is not necessary to protect privacy. In its 2012 Privacy Report, which set forth recommended best practices, the Commission stated that companies should not be compelled to provide choice before collecting and using consumer data for practices that are consistent with the context of a transaction or the company's relationship with the consumer. Indeed, because these data uses are generally consistent with consumers' reasonable expectations, the cost to consumers and businesses of providing notice and choice likely outweighs the benefits.[160] This principle applies equally to the Internet of Things.

For example, suppose a consumer buys a smart oven from ABC Vending, which is connected to an ABC Vending app that allows the consumer to remotely turn the oven on to the setting, "Bake at 400 degrees for one hour." If ABC Vending decides to use the consumer's oven-usage information to improve the sensitivity of its temperature sensor or to recommend another of its products to the consumer, it need not offer the consumer a choice for these uses, which are consistent with its relationship with the consumer. On the other hand, if the oven manufacturer shares a consumer's personal data with, for example, a data broker or an ad network, such sharing would be inconsistent with the context of the consumer's relationship with the manufacturer, and the company should give the consumer a choice. The practice of distinguishing contextually appropriate data practices from those that are inconsistent with

[160] Privacy Report, *supra* note 85, at 38-39; *id.* at 38 ("The Commission believes that for some practices, the benefits of providing choice are reduced – either because consent can be inferred or because public policy makes choice unnecessary.").

context reduces the need for companies to provide opportunities for consumer choice before every single data collection.

Staff acknowledges the practical difficulty of providing choice when there is no consumer interface, and recognizes that there is no one-size-fits-all approach. Some options – several of which were discussed by workshop participants – include the following:

- **Choices at point of sale:**
  One auto industry participant noted that his company provides consumers with opt-in choices at the time of purchase in "[p]lain language and multiple choices of levels."[161]

- **Tutorials:**
  Facebook offers a video tutorial to guide consumers through its privacy settings page. IoT device manufacturers can offer similar vehicles for explaining and providing choices to consumers.

- **Codes on the device:**
  Manufacturers could affix a QR code or similar barcode that, when scanned, would take the consumer to a website with information about the applicable data practices and enable consumers to make choices through the website interface.[162]

- **Choices during set-up:**
  Many IoT devices have an initial set-up wizard, through which companies could provide clear, prominent, and contextual privacy choices.

[161] Remarks of Kenneth Wayne Powell, Toyota Technical Center ("Powell"), Transcript of Workshop at 278.

[162] *See* Article 29 Working Group Opinion, *supra* note 55, at 18 (proposing that a "device manufacturer could print on things equipped with sensors a QR code, or a flashcode describing the type of sensors and the information it captures as well as the purposes of these data collections").

- **Management portals or dashboards:**[163]
  In addition to the availability of initial set-up choices, IoT devices could also include privacy settings menus that consumers can configure and revisit. For example, in the mobile context, both Apple and Google (for Android) have developed dashboard approaches that seem promising – one that is framed by data elements, such as geolocation and contacts (Apple), and one that is framed by individual apps (Android).[164] Similarly, companies developing "command centers" for their connected home devices[165] could incorporate similar privacy dashboards. Properly implemented, such "dashboard" approaches can allow consumers clear ways to determine what information they agree to share.

- **Icons:**
  Devices can use icons to quickly convey important settings and attributes, such as when a device is connected to the Internet, with a toggle for turning the connection on or off.

- **"Out of Band" communications requested by consumers:**
  When display or user attention is limited, it is possible to communicate important privacy and security settings to the user via other channels. For example, some home appliances allow users to configure their devices so that they receive important information through emails or texts.

- **General Privacy Menus:**
  In addition to the types of specific settings and choices described above, devices and their associated platforms could enable consumers to aggregate choices into "packets." [166] This could involve having more general settings like "low privacy," "medium," or "high," accompanied by a clear and conspicuous explanation of the settings.

- **A User Experience Approach:**
  One participant noted that companies could consider an approach that applies learning from consumer behavior on IoT devices, in order to personalize choices.[167] For example, a manufacturer that offers two or more devices could use the consumer's preferences on one device (*e.g.*, "do not transmit any of my information to third parties") to set a default preference on another. As another example, a single device, such as a home appliance "hub" that stores data locally – say on the consumer's home network – could learn a consumer's preferences based on prior behavior and predict future privacy preferences as new appliances are added to the hub.

---

[163] *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 6.

[164] *See* Mobile Disclosures Report, *supra* note 96, at 16-17.

[165] Don Clark, *The Race to Build Command Centers for Smart Homes*, WALL ST. J. (Jan. 4, 2015), *available at* http://www.wsj.com/articles/the-race-to-build-command-centers-for-smart-homes-1420399511.

[166] Remarks of Joseph Lorenzo Hall, Center for Democracy & Technology ("Hall"), Transcript of Workshop at 216.

[167] Remarks of Nguyen, Transcript of Workshop at 48.

Of course, whatever approach a company decides to take, the privacy choices it offers should be clear and prominent, and not buried within lengthy documents.[168] In addition, companies may want to consider using a combination of approaches.

Staff also recognizes concerns discussed at the workshop[169] and, as noted above, in the White House Big Data Report and PCAST Report that, applied aggressively, a notice and choice approach could restrict unexpected new uses of data with potential societal benefits. For this reason, staff has incorporated certain elements of the use-based model into its approach. For instance, the idea of choices being keyed to context takes into account how the data will be used: if a use is consistent with the context of the interaction – in other words, it is an expected use – then a company need not offer a choice to the consumer. For uses that would be inconsistent with the context of the interaction (*i.e.*, unexpected), companies should offer clear and conspicuous choices. Companies should not collect sensitive data without affirmative express consent.

In addition, if a company enables the collection of consumers' data and de-identifies that data immediately and effectively, it need not offer choices to consumers about this collection. As noted above, robust de-identification measures can enable companies to analyze data they collect in order to innovate in a privacy-protective way.[170] Companies can use such de-identified data without having to offer consumers choices.

---

[168] This discussion refers to how companies should communicate choices to consumers. Lengthy privacy policies are not the most effective consumer communication tool. However, providing disclosures and choices through these privacy policies serves an important accountability function, so that regulators, advocacy groups, and some consumers can understand and compare company practices and educate the public. *See* Privacy Report, *supra* note 85, at 61-64.

[169] *See, e.g., Comment of Future of Privacy Forum*, #510 cmt. #00013, App. A at 9; *Comment of GS1 US*, #484 cmt. #00030 at 5; *Comment of Software & Info. Indus. Ass'n.*, #484 cmt. #00025 at 6-9.

[170] *See, e.g.*, Comment of CTIA – The Wireless Ass'n, #484 cmt. #00009 at 10-11; Comment of Future of Privacy Forum, #510 cmt. #00013 at 5.

Staff also notes that existing laws containing elements of the use-based approach apply to the IoT. The FCRA sets forth a number of statutory protections applicable to "consumer report" information, including restrictions on the uses for which this information can be shared.[171] Even when there is a permissible use for such information, the FCRA imposes an array of protections, including those relating to notice, access, disputes, and accuracy.[172] In addition, the FTC has used its "unfairness" authority to challenge a number of harmful uses of consumer data. For example, in the agency's recent case against Leap Lab, the Commission alleged that defendants sold consumer payday loan applications that included consumers' Social Security and financial account numbers to non-lenders that had no legitimate need for this sensitive personal information.[173]

Staff has concerns, however, about adopting solely a use-based model for the Internet of Things. First, because use-based limitations have not been fully articulated in legislation or other widely-accepted multistakeholder codes of conduct, it is unclear who would decide which additional uses are beneficial or harmful.[174] If a company decides that a particular data use is beneficial and consumers disagree with that decision, this may erode consumer trust. For example, there was considerable consumer outcry over Facebook's launch of the Beacon service,

---

[171] FCRA, 15 U.S.C. § 1681–1681v. Section 604 of the FCRA sets forth the permissible purposes for which a consumer reporting company may furnish consumer report information, such as to extend credit or insurance or for employment purposes. 15 U.S.C. 1681b.

[172] FCRA, 15 U.S.C. § 1681–1681v.

[173] Press Release, FTC, FTC Charges Data Broker with Facilitating the Theft of Millions of Dollars from Consumers' Accounts (Dec. 23, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/12/ftc-charges-data-broker-facilitating-theft-millions-dollars.

[174] ANN CAVOUKIAN ET AL., INFO. & PRIVACY COMM'R, ONT., CAN., THE UNINTENDED CONSEQUENCES OF PRIVACY PATERNALISM (2014), *available at* http://www.privacybydesign.ca/content/uploads/2014/03/pbd-privacy_paternalism.pdf.

as well as Google's launch of the Buzz social network, which ultimately led to an FTC enforcement action.[175]

Second, use limitations alone do not address the privacy and security risks created by expansive data collection and retention. As explained above, keeping vast amounts of data can increase a company's attractiveness as a data breach target, as well as the risk of harm associated with any such data breach. For this reason, staff believes that companies should seek to reasonably limit the data they collect and dispose of it when it is no longer needed.

Finally, a use-based model would not take into account concerns about the practice of collecting sensitive information.[176] Consumers would likely want to know, for example, if a company is collecting health information or making inferences about their health conditions, even if the company ultimately does not use the information.[177]

---

[175] *See, e.g.*, Google Inc., No. C-4336 (Oct. 13, 2011) (consent order), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf.

[176] In addition to collecting sensitive information outright, companies might create sensitive information about consumers by making inferences from other data that they or others have already collected. A use-based model might not address, or provide meaningful notice about, sensitive inferences. The extent to which a use-based model limits or prohibits sensitive inferences will depend on how the model defines harms and benefits and how it balances the two, among other factors.

[177] Of course, if a company misstates how it uses data, this could be a deceptive practice under Section 5 of the FTC Act. The FTC has brought cases against companies that promise to use consumers' data one way, but used it in another way. *See, e.g.*, Google Inc., *supra* note 175. The FTC can also use its unfairness authority to prohibit uses of data that cause or are likely to cause substantial injury to a consumer, where that injury was not reasonably avoidable by the consumer, and where the injury was not outweighed by a benefit to consumers or competition. *See, e.g.*, Designerware, LLC, No. C-4390 (Apr. 11, 2013) (consent order) (alleging that installing and turning on webcams on people's home computers without their knowledge or consent was an unfair practice), *available at* http://www.ftc.gov/enforcement/cases-proceedings/112-3151/designerware-llc-matter.

The establishment of legislative or widely-accepted multistakeholder use-based frameworks could potentially address some of these concerns and should be considered. For example, the framework could set forth permitted or prohibited uses. In the absence of such legislative or widely accepted multistakeholder frameworks, however, the approach set forth here – giving consumers information and choices about their data – continues to be the most viable one for the IoT in the foreseeable future.

Legislation

Summary of Workshop Discussions

Workshop participants discussed whether legislation is needed to ensure appropriate protections for data collected through connected devices. Some participants expressed trepidation that the benefits of the IoT might be adversely affected should policymakers enact laws or regulations on industry.[178] One participant stated, "[t]he FTC should be very cautious about proposing regulation of this sector, given its importance to innovation in America."[179] Another participant noted that "we should be careful to kind of strike a balance between guiding companies in the right direction and enforcing."[180] Still another worried that the workshop might "represent[] the beginning of a regulatory regime for a new set of information technologies that are still in their infancy" and advised policymakers to "exercise restraint and avoid the impulse to regulate before serious harms are demonstrated."[181] Another participant questioned what legislation would look like, given the difficulty of defining the contours of privacy rights.[182]

A number of participants noted that self-regulation is the appropriate approach to take to the IoT. One participant stated, "self-regulation and best business practices – that are technology

[178] *See, e.g.*, *Comment of Direct Mktg. Ass'n*, #484 cmt. #00010.

[179] *Comment of Internet Commerce Coal.*, #484 cmt. #00020 at 2.

[180] Remarks of Rogers, Transcript of Workshop at 359.

[181] *Comment of Tech. Policy Program of the Mercatus Ctr., George Mason Univ.*, #484 cmt. #00024 at 1 and 9.

[182] Remarks of Cerf, Transcript of Workshop at 149-50 ("Well, I have to tell you that regulation is tricky. And I don't know, if somebody asked me, would you write a regulation for this, I would not know what to say. I don't think I have enough understanding of all of the cases that might arise in order to say something useful about this, which is why I believe we are going to end up having to experience problems before we understand the nature of the problems and maybe even the nature of the solutions.").

neutral – along with consumer education serve as the preferred framework for protecting consumer privacy and security while enhancing innovation, investment, competition, and the free flow of information essential to the Internet of Things."[183] Another participant agreed, stating "[s]elf-regulatory regimes have worked well to ensure consumer privacy and foster innovation, and industry has a strong track record of developing and implementing best practices to protect information security."[184]

Other participants noted that the time is ripe for legislation, either specific to the IoT or more generally.[185] One participant who called for legislation noted that the "explosion of fitness and health monitoring devices is no doubt highly beneficial to public health and worth encouraging," but went on to state:

> At the same time, data from these Internet of Things devices should not be usable by insurers to set health, life, car, or other premiums. Nor should these data migrate into employment decisions, credit decisions, housing decisions, or other areas of public life. To aid the development of the Internet of Things—and reap the potential public health benefits these devices can create—we should reassure the public that their health data will not be used to draw unexpected inferences or incorporated into economic decisionmaking.[186]

Recommendations

The Commission staff recognizes that this industry is in its relatively early stages. Staff does not believe that the privacy and security risks, though real, need to be addressed through IoT-specific legislation at this time. Staff agrees with those commenters who stated that there is

---

[183] *Comment of U.S. Chamber of Commerce*, #510 cmt. #00011 at 3.

[184] *Comment of Consumer Elec. Ass'n*, #484 cmt. #00027 at 18.

[185] Remarks of Hall, Transcript of Workshop at 180-81 (supporting baseline privacy legislation); *see also* Remarks of Jacobs, Transcript of Workshop at 360 (emphasizing importance of enforcement "in the meantime").

[186] Peppet, *Regulating the Internet of Things*, *supra* note 62, at 151.

great potential for innovation in this area, and that legislation aimed specifically at the IoT at this stage would be premature. Staff also agrees that development of self-regulatory programs[187] designed for particular industries would be helpful as a means to encourage the adoption of privacy- and security-sensitive practices.

However, while IoT specific-legislation is not needed, the workshop provided further evidence that Congress should enact general data security legislation. As noted above, there was wide agreement among workshop participants about the importance of securing Internet-enabled devices, with some participants stating that many devices now available in the market are not reasonably secure, posing risks to the information that they collect and transmit and also to information on consumers' networks or even to others on the Internet.[188] These problems highlight the need for substantive data security and breach notification legislation at the federal level.

The Commission has continued to recommend that Congress enact strong, flexible, and technology-neutral legislation to strengthen the Commission's existing data security enforcement tools and require companies to notify consumers when there is a security breach. Reasonable and appropriate security practices are critical to addressing the problem of data breaches and protecting consumers from identity theft and other harms. Notifying consumers of breaches after they occur helps consumers protect themselves from any harm that is likely to be caused by the misuse of their data. These principles apply equally to the IoT ecosystem.[189]

---

[187] Remarks of Lightner, Transcript of Workshop at 56-57 (discussing voluntary code of conduct for energy data); *Comment of Future of Privacy Forum*, #484 cmt. #00013 (discussing self-regulatory efforts in a variety of contexts).

[188] *See* discussion *supra* pp. 10-14 and accompanying notes.

[189] One commenter argued that breach notification laws should be even broader in the IoT context. *See* Remarks of Peppet, Transcript of Workshop at 220 (urging that breach notification laws be extended for the IoT to cover additional types of information that would lead to consumer harm but would not meet the definition of personal

We emphasize that general technology-neutral data security legislation should protect against unauthorized access to both personal information and device functionality itself. The security risks associated with IoT devices, which are often not limited to the compromise of personal information but also implicate broader health and safety concerns, illustrate the importance of these protections. For example, if a pacemaker is not properly secured, the concern is not merely that health information could be compromised, but also that a person wearing it could be seriously harmed.[190] Similarly, a criminal who hacks into a car's network could cause a car crash. Accordingly, general data security legislation should address risks to both personal information and device functionality.

In addition, the pervasiveness of information collection and use that the IoT makes possible reinforces the need for baseline privacy standards.[191] Commission staff thus again recommends that Congress consider enacting broad-based (as opposed to IoT-specific) privacy legislation. Such legislation should be flexible and technology-neutral, while also providing clear rules of the road for companies about such issues as when to provide privacy notices to consumers and offer them choices about data collection and use practices. Although the Commission currently has authority to take action against some IoT-related practices, it cannot

---

information protected under existing laws). The Commission has not taken a position on such an approach at this time.

[190] Andrea Peterson, *Yes, Terrorists Could Have Hacked Dick Cheney's Heart*, WASH. POST (Oct. 21, 2013), http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/.

[191] Commissioner Ohlhausen disagrees with this portion of the staff's recommendation. She believes that the FTC's current Section 5 authority to prohibit unfair and deceptive acts or practices already requires notice and choice for collecting sensitive personally identifiable information and protects against uses of consumer information that cause or are likely to cause substantial consumer harm not outweighed by benefits to consumers or competition. Furthermore, the FCRA, HIPAA, and other laws already provide additional sector-specific privacy protections. Thus, Commissioner Ohlhausen questions what harms baseline privacy legislation would reach that the FTC's existing authority cannot.

mandate certain basic privacy protections – such as privacy disclosures or consumer choice – absent a specific showing of deception or unfairness.

The Commission has issued a report and testified before Congress calling for baseline federal privacy legislation.[192] These recommendations have been based on concerns about the lack of transparency regarding some companies' data practices and the lack of meaningful consumer control of personal data. These concerns permeate the IoT space, given the ubiquity of information collection, the broad range of uses that the IoT makes possible, the multitude of companies involved in collecting and using information, and the sensitivity of some of the data at issue.

Staff believes such legislation will help build trust in new technologies that rely on consumer data, such as the IoT. Consumers are more likely to buy connected devices if they feel that their information is adequately protected.[193] A 2012 survey shows, for example, that a majority of consumers uninstalled an app because they were concerned that it was collecting too much personal information, or declined to install an app at all.[194] A 2014 survey shows that 87% of consumers are concerned about the type of data collected through smart devices, and 88% of

---

[192] *See, e.g.*, Privacy Report, *supra* note 85, at 12-13; *The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission Before the S. Comm. On Commerce, Science & Transportation* (May 9, 2012) (statement of FTC), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-need-privacy-protections-perspectives-administration-and/120509privacyprotections.pdf.

[193] Remarks of Chibba, Transcript of Workshop at 312-13; *see also* Remarks of Wolf, Transcript of Workshop at 260 (noting that "the Michigan Department of Transportation and the Center for Automotive Research identified security as the primary concern for connected car technologies"); *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 5 ("If there are lax controls and insufficient oversight over the collection of personal information through connected devices, consumers will lose trust in the evolving technologies. Even with proper controls and oversight, helping consumers understand the benefits from these innovations and the protections in place is important lest they feel that personal control has been sacrificed for corporate gain.").

[194] JAN LAUREN BOYLES ET AL., PEW INTERNET PROJECT, PRIVACY AND DATA MANAGEMENT ON MOBILE DEVICES (2012), *available at* http://www.pewinternet.org/files/old-media//Files/Reports/2012/PIP_MobilePrivacyManagement.pdf.

consumers want to control the data that is collected through smart devices.[195] Surveys also show that consumers are more likely to trust companies that provide them with transparency and choices.[196] General privacy legislation that provides for greater transparency and choices could help both consumers and businesses by promoting trust in the burgeoning IoT marketplace.

In addition, as demonstrated at the workshop, general privacy legislation could ensure that consumers' data is protected, regardless of who is asking for it. For example, workshop participants discussed the fact that HIPAA protects sensitive health information, such as medical diagnoses, names of medications, and health conditions, but only if it is collected by certain entities, such as a doctor's office or insurance company.[197] Increasingly, however, health apps are collecting this same information through consumer-facing products, to which HIPAA protections do not apply. Commission staff believes that consumers should have transparency and choices over their sensitive health information, regardless of who collects it. Consistent standards would also level the playing field for businesses.

---

[195] The TRUSTe Internet of Things Privacy Index, 2014 U.S. Edition, *available at* http://www.truste.com/us-internet-of-things-index-2014/.

[196] *See, e.g.*, Adam DeMartino, Evidon, *RESEARCH: Consumers Feel Better About Brands that Give Them Transparency and Control Over Ads* (Nov. 10, 2010), *available at* http://www.evidon.com/blog/research-consumers-feel-better-about-brands-that-give-them-transparency-and-control-over-ads; Scott Meyer, *Data Transparency Builds Trust*, BRANDREPUBLIC (Oct. 31, 2012), *available at* http://www.brandrepublic.com/news/1157134/; TRUSTe, *New TRUSTe Survey Finds Consumer Education and Transparency Vital for Sustainable Growth and Success of Online Behavioral Advertising* (July 25, 2011), *available at* http://www.truste.com/about-TRUSTe/press-room/news_truste_behavioral_advertising_survey_2011.

[197] Remarks of Hall, Transcript of Workshop at 179; Remarks of T. Drew Hickerson, Happtique, Transcript of Workshop at 350; *Comment of Ctr. for Democracy & Tech*, #510 cmt. #00016 at 12.

While Commission staff encourages Congress to consider privacy and security legislation, we will continue to use our existing tools to ensure that IoT companies continue to consider security and privacy issues as they develop new devices and services. Specifically, we will engage in the following initiatives:

- **Law enforcement:**
  The Commission enforces the FTC Act, the FCRA, the Children's Online Privacy Protection Act, the health breach notification provisions of the HI-TECH Act, and other laws that might apply to the IoT. Where appropriate, staff will recommend that the Commission use its authority to take action against any actors it has reason to believe are in violation of these laws. The TRENDNet case, discussed above, was the Commission's first IoT case. We will continue to look for cases involving companies making IoT devices that, among other things, do not maintain reasonable security, make misrepresentations about their privacy practices, or violate the requirements of the FCRA when they use information for credit, employment, insurance, or other eligibility decisions. Staff believes that a strong FTC law enforcement presence will help incentivize appropriate privacy and security-protective practices by companies manufacturing and selling connected devices.

- **Consumer and business education:**
  Consumers should understand how to get more information about the privacy of their IoT devices, how to secure their home networks that connect to IoT devices, and how to use any available privacy settings. Businesses, and in particular small businesses, would benefit from additional information about how to reasonably secure IoT devices. The Commission staff will develop new consumer and business education materials in this area.

- **Participation in multi-stakeholder groups:**
  Currently, Commission staff is working with a variety of groups that are considering guidelines related to the Internet of Things. For example, staff participates in NTIA's multi-stakeholder group that is considering guidelines for facial recognition and the Department of Energy's multi-stakeholder effort to develop guidelines for smart meters. Even in the absence of legislation, these efforts can result in best practices for companies developing connected devices, which can significantly benefit consumers. Commission staff will continue to participate in multistakeholder groups to develop guidelines related to the IoT.

- **Advocacy:**
  Finally, where appropriate, the Commission staff will look for advocacy opportunities with other agencies, state legislatures, and courts to promote protections in this area. Among other things, staff will share the best practices discussed in this report with other government entities in order to ensure that they consider privacy and security issues.

Conclusion

The IoT presents numerous benefits to consumers, and has the potential to change the ways that consumers interact with technology in fundamental ways. In the future, the Internet of Things is likely to meld the virtual and physical worlds together in ways that are currently difficult to comprehend. From a security and privacy perspective, the predicted pervasive introduction of sensors and devices into currently intimate spaces – such as the home, the car, and with wearables and ingestibles, even the body – poses particular challenges. As physical objects in our everyday lives increasingly detect and share observations about us, consumers will likely continue to want privacy. The Commission staff will continue to enforce laws, educate consumers and businesses, and engage with consumer advocates, industry, academics, and other stakeholders involved in the IoT to promote appropriate security and privacy protections. At the same time, we urge further self-regulatory efforts on IoT, along with enactment of data security and broad-based privacy legislation.