KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

January 10, 2014

Federal Trade Commission
600 Pennsylvania Avenue N.W.
Room H-113 (Annex B)
Washington, DC 20580

Re: Comments after November 2013 Workshop on the "Internet of Things"

The Center for Democracy & Technology[1] (CDT) is pleased to submit comments in response to the Federal Trade Commission's (FTC) call for submissions[2] on the privacy and security aspects of the Internet of Things (IoT) in light of the material presented and discussion at the FTC's November 21, 2013 workshop.

In our comments we make a few crucial points. First, there are challenging privacy and security concerns in IoT systems that the FTC cannot ignore. Second, Fair Information Practice Principles (FIPPs) are only more relevant in an IoT environment; the complexity that comes with increased sensor- and internet-enabled devices cannot be used to justify hidden, unbounded, and comprehensive data collection by all device manufacturers without a consumer's insight or control. Finally, we discuss health-specific applications of IoT, from which we can draw more general principles about applying FIPPs to IoT devices and systems.

I. The Internet of Things Poses Acute Privacy and Security Challenges

A recent article that surveyed definitions of IoT acknowledged that there was no agreed-upon definition of the term and identified the following definition as the best one available because of its broadness and descriptiveness: "The Internet of Things allows people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service."[3] As indicated by this definition, data collection, and human interaction in an IoT

[1] CDT is a non-profit Internet and technology advocacy organization working to keep the Internet and digital life open, free, and innovative. CDT promotes public policies that preserve privacy,

[2] FED. TRADE COMM'N, *Internet of Things: Privacy and Security in a Connected World*, http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-and-security-connected-world

[3] Charith Perera, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos, *Context Aware Computing for The Internet of Things: A Survey*, IEEE Comm. Surv. & Tutorials J. 99, 1–4 (2013).

environment is meant to be seamless, with as little fuss as needed for a given device to function. This naturally leads to a few challenging consequences for privacy and security.

Data collection and interaction with IoT systems can easily be out of context for consumers. For example, when a smart television uses voice or face recognition to personalize the user experience, it can also easily measure signals in its surrounding environment — e.g., a living room — that have nothing to do with entertainment.[4] For example, it may be able to determine how often a family plays board games, or record the conversation of a phone call that takes place in the living room without the knowledge of the user.

While large complex smart IoT devices like televisions will have WiFi connections, software updates, and multiple types of functionality and interfaces, we expect many of the more widely deployed IoT systems will be more modest, without such capabilities. These devices will be cheap, even disposable, and the incentives for the manufacturer to provide regular security updates will be minimal. Such incentives have failed certain elements of the smart phone market, resulting in millions of vulnerable devices that will remain so for the remainder of their shelflife.[5] Thus, we expect to see entirely new types of market events, such as product recalls, based solely on vulnerabilities in the network and computational interface that provide IoT-like communication services. Certainly many of these devices and systems may never be updated in their after-market environment, and home networks and IoT-capable communication platforms will have to be designed to deal with errant and outright hostile (e.g., hacked through a flaw or vulnerability) participants on the local network.

The user interface on such devices may be very simple to non-existent, making interaction with the user difficult. Interfaces are critical for configuration of user controls and for providing notice and accepting consent. These properties, as we discuss below, will have to shift to other elements of the IoT environment, either within the network itself or physical features of the device in non-traditional interface elements (e.g., a pull-tab on a IoT milk carton that renders network functionality inoperable).

Further, setting up network access on such devices will likely be difficult and they may not have the power to drive more advanced networking protocols such as WiFi, Bluetooth, or cellular networking. Therefore, we expect IoT-enabled platforms that mediate large quantities of low-power and RFID/NFC-enabled devices — which, instead of using on-board power, use the RF signal itself to power computation and network circuitry — to come into play. This raises many of the concerns we have with comprehensive collection: to the extent that a

[4] Gary Merson, *Is Your TV Watching You? Latest Models Raise Concerns*, NBC News Technology Blog (March 19, 2012, 10:46 AM), http://www.nbcnews.com/technology/your-tv-watching-you-latest-models-raise-concerns-483619.

[5] Dan Goodin, *ACLU Asks Feds to Probe Wireless Carriers over Android Security Updates*, Ars Technica (April 17, 2013, 10:01 PM), http://arstechnica.com/security/2013/04/wireless-carriers-deceptive-and-unfair/.

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.

This is a feature of likely IoT system deployments that we must emphasize: many of the concerns that apply to in-the-home monitoring devices like smart grid technologies[6] will apply to IoT. IoT systems will in most cases be sensing platforms augmenting devices and objects in the home or in businesses. Light sensors can tell how often certain rooms are occupied at night or how often the refrigerator is opened, depending on which objects they are located. Temperature sensors may be able to tell when one bathes, exercises, or leaves the home entirely. Microphones can easily pick up the content of conversations in the home and, with enough fidelity, can identify who is speaking. In essence, the privacy and security concerns we've highlighted in the section are made only more serious and concerning given the likely home and office deployments of IoT systems.

II. Fair Information Practices and IoT

The Federal Trade Commission should emphasize that the Fair Information Practice Principles all still apply in a technological environment of increased data collection and connectivity. Indeed, the greater potential for privacy violations requires a more rigorous application of these time-honored concepts.

There is nothing intrinsically magical about the Internet of Things: the primary features are simply increased surveillance capabilities and Internet connectivity from devices consumers don't normally think of as having those abilities. These "smart" devices clearly offer consumers positive benefits, but the value they offer does not trump the FIPPs. To the contrary, the FIPPs exist to ensure that users get what they want out of these new products.

Some have posed the question of how the FTC should address IoT as a binary choice: either prohibit emerging technologies unless they can prove that they will not cause harm (the "precautionary principle") or allow new products to emerge without interference ("permissionless innovation").[7] We believe that this dichotomy presents a false choice. Instead, the FTC should aggressively enforce Section 5 as applied to the Internet of Things as it has for all other technologies.[8] We also believe that otherwise unregulated entities should not have to affirmatively solicit FTC permission to offer consumers new products and

[6] CTR. FOR DEMOCRACY & TECH. & ELEC. FRONTIER FOUND., "Proposed Smart Grid Privacy Policies and Procedures," before The Public Utilities Commission of the State of California (December 18, 2008), *available at* https://cdt.org/files/pdfs/CDT_EFF_PoliciesandProcedures_15Oct2010_OpeningComment_1.pdf.

[7] MERCATUS CTR., *Privacy and Security Implications of the Internet of Things* (May 31, 2013), *available at* http://mercatus.org/publication/privacy-and-security-implications-internet-things.

[8] TrendNet Inc., File No. 1223090 (Fed. Trade Comm'n Sept. 2009) (decision and order), http://www.ftc.gov/sites/default/files/documents/cases/2013/09/130903trendnetorder.pdf.

offerings. However, if they violate the FTC's long-standing principles that enable informed consumer choice and control, they should be subject to robust enforcement. Novelty should not be used as a defense to data practices that run contrary to a consumer's reasonable expectations in appropriate flows of data that remain within the context of their understanding of a product.

Others have advanced the notion that the proliferation of connected sensors — the combination of the Internet of Things and Big Data — means that there is too much information for users to control. As such, they argue that user control should play less or no role in information governance. These commentators seek to essentially strip the FIPPs down to two bare concepts: corporate accountability and some undefined limitations of harmful uses. We believe that these comments have it backward. The increased data capabilities stemming from the Internet of Things means that users deserve an even more robust application of all the FIPPs, including *stronger* and *more effective* controls that rise to the challenges of saturated information and interaction environments like those envisioned in the Internet of Things. Use limitation and corporate accountability are not by themselves sufficient — organizations are not perfect, as demonstrated by the FTC's substantial track record of enforcement against large companies with very mature data governance programs. Moreover, even theoretically perfect accountability programs cannot protect against all threat models.[9]

The fundamental technology behind the Internet of Things is not new — connected devices have existed for years. What is different is the scope — it's not just three or four connected devices, it's potentially a dozen or more — and the saturation of such devices in private locations such as the home and office. But consumers have reasonable expectations today about the limits of what their smart devices collect about them. We do not expect our phone or computer to transmit to device manufacturers a log of all the things that we do. If we affirmatively sign up for a cloud-based service (such as a health analytics service like FitBit), we expect to have control over what gets collected and with whom it gets shared. ***However, the complexity that comes with increased sensor- and internet-enabled devices cannot be used to justify hidden, unbounded, and comprehensive data collection by all device manufacturers without a consumer's insight or control***. The rules — that is, the FIPPs — that have governed traditional connected devices should govern the new technologies as well. Just because a computer-leasing company has the capacity to remotely turn on a webcam and upload footage without informed prior consent does not mean that the company should do so.[10] Similarly, other, new smart devices that

[9] Justin Brookman & G.S. Hans, *Why Collection Matters: Surveillance as a De Facto Privacy Harm*, FUTURE OF PRIVACY F., *available at* http://www.futureofprivacy.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf.

[10] DesignerWare LLC., File No. 1223151, Docket No. C-4390 (Fed. Trade Comm'n Apr. 11, 2013) (decision and order), http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415designerwaredo.pdf

inherently have the ability to surveil users should not necessarily presume to do so in the name of Big Data. Ultimately, the choice must reside with the consumer.

A. Purpose Specification/Use Limitation/Notice and Transparency

The core concepts of notice, transparency, purpose specification, and use limitation all clearly apply to the Internet of Things. Companies should absolutely inform consumers what they're doing with their data, and not use or sell their data for undisclosed purposes.

Certainly, the increased data collection and connectivity involved in IoT means that there is potentially more that should be conveyed to consumers. However, the FTC's existing standards for notice and transparency should apply to these new technologies just as they do for existing technologies. A company should have an affirmative obligation to clearly and conspicuously disclose important data flows to a user — outside of a privacy policy.[11] Failure to prominently point out an unintuitive but significant data collection/use/transfer practice should constitute a material omission, and would be a deceptive and unfair practice under Section 5 of the FTC Act.[12]

That said, not all data collection practices can or should be disclosed up front. But at the very least, companies should make available *somewhere* what exactly they are doing with user data. For information practices that do not rise to needing to be disclosed clearly and conspicuously, companies should be obligated to meaningfully describe these practices within a privacy policy. This transparency allows advocates, regulators, and interested consumers to hold companies accountable for their practices. Unfortunately, there has been a trend among some companies of making their privacy policies so vague as to be inscrutable.[13] This is done in part to avoid accountability for potentially unpopular practices, but also to avoid committing a deceptive practice in violation of Section 5 of the FTC Act. A narrow interpretation of Section 5 as a mere prohibition on false statements creates perverse incentives for companies to disclose very little

[11] FED. TRADE COMM'N, *Mobile Privacy Disclosures: Building Trust through Transparency* (Feb. 2013) at 23-24, *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; FEDERAL TRADE COMMISSION, *.com Disclosures: How to Make Effective Disclosures in Digital Advertising* (March 2013) at 7, *available at* http://www.business.ftc.gov/sites/default/files/pdf/bus41-dot-com-disclosures-information-about-online-advertising.pdf; Sears Holding Mgmt. Corp., File No. 0823099, Docket No. C-4264 (Fed. Trade Comm'n Aug. 31, 2009) (complaint), http://www.ftc.gov/sites/default/files/documents/cases/2009/09/090604searscmpt.pdf.

[12] Sears Holding Mgmt. Corp., File No. 0823099, Docket No. C-4264 (Fed. Trade Comm'n Aug. 31, 2009) (complaint), http://www.ftc.gov/sites/default/files/documents/cases/2009/09/090604searscmpt.pdf; DesignerWare, LLC. File No. 1123151 (Fed. Trade Comm'n August 2012), http://www.ftc.gov/sites/default/files/documents/cases/2012/09/120925designerwarecmpt.pdf.

[13] Casey Johnston, *Snapchat's Bad Security Shows How Data Use Policies Fail*, Ars Technica (Jan. 6, 2014, 10:59 AM), http://arstechnica.com/tech-policy/2014/01/snapchats-bad-security-shows-how-data-use-policies-fail/.

about specific data processing activities. The less a company says in a privacy policy, the less likely it is to make a false statement. For that reason, we strongly support the recent trend in FTC enforcement actions to classify failure to describe specific behaviors within a privacy policy as a *deceptive omission* in violation of Section 5.[14]

It may not be practical or possible to describe every future application of user data within a privacy policy (this problem is not specific to the Internet of Things, but more to the issue of Big Data generally). For that reason, we are supportive of the idea of *context* introduced in the White House report on consumer privacy: that if a new use of data is contextually related to the reason the data was supplied in the first place, a company should not need to seek new permission for that related behavior.[15] However, that does not mean that any and all data usages can be covered by listing categories within a privacy policy such as "product improvement," "research," or "sharing with trusted third parties." These statements are no more illuminating than a provision in a contract stating, "you agree to pay a price for this service as subsequently determined."[16] Such statements of purpose are so vague as to be illusory, and consumers cannot be understood to have consented to anything so ethereal.

On the other hand, product manufacturers can clearly state to a user that they will collect a wide range of information from the user in order to provide tailored suggestions or advertisements in the future. Google Now is a good example of such a product: Google tells the user that a broad range of Google information, including geolocation, is going to be collected in order to provide suggestions and tips going forward — such as an alarm telling you when you need to leave for the airport based on your schedule and current traffic patterns. This value proposition is not entirely explicit — indeed, the company notes that it will continue to iterate on what services to provide — but the basic contours of the arrangement are clear to the consumer. There is a meeting of the minds over what data the company is collecting and how they use that data on behalf of the consumer. On the other hand, it would be out of context for, say, a phone's handset maker (e.g. Samsung) from doing the precise same thing by default without the user's knowledge or permission.

B. Data Minimization and Security

We strongly urge the FTC to emphasize that the concept of data minimization is still valid in the age of the Internet of Things and Big Data. Certainly, the core

[14] Goldenshores Tech. LLC, File No. 1323087 (Fed. Trade Comm'n Dec. 05, 2013) (complaint) http://www.ftc.gov/sites/default/files/documents/cases/131205goldenshorescmpt.pdf; G.S. Hans, *Goldenshores Case Demonstrates Flaws in Current Mobile Privacy Practices*, Center for Democracy PolicyBeta (Dec. 23, 2013), https://www.cdt.org/blogs/gs-hans/2312goldenshores-case-demonstrates-flaws-current-mobile-privacy-practices.

[15] White House, *Consumer Data Privacy in a Networked World* at 17 (Feb. 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[16] Douglas v. U.S. Dist. Court ex rel Talk America, 495 F.3d 1062 (9th Cir. 2007).

notion should be indisputable — you shouldn't collect data that you don't need, and you shouldn't keep data that you don't need anymore.

Of course, whether data is *needed* is tied to the previous discussion of purpose specification — if vague, inscrutable purposes such as "product improvement" and "research" are cognizable, then any and all data can be deemed necessary for some as-yet-unknown future data application. However, we urge the FTC to reject the notion that "we might eventually find a use for the data" constitutes a sufficient specification of purpose for data collection and retention. At some point, the marginal value to retaining data will be outweighed by, *inter alia*, the risk that the data will be breached or otherwise compromised.[17] Companies should be encouraged (at the very least) to disclose data retention periods in order to allay concerns about overbroad retention and the possibility of data breaches.

Security will likely be a particular problem in the IoT world, as more and more (and less and less sophisticated) companies possess the capacity to collect and retain a wide range of personal information.[18] The FTC should stress to companies that they will continue to be held accountable for failing to safeguard the data they maintain, and that failure to purge old data will be an indepedent factor in evaluating whether a company's data security practices were reasonable. The FTC should relatedly make clear that merely holding onto data needlessly is an element that will be considered when evaluating whether data security practices are unfair under Section 5.

1. Security updates

The Commission has posed the question of how a company can deliver necessary security updates to consumers if they do not have an ongoing relationship with its users. We do not believe there is a meaningful conflict here. Today, companies deliver updates to operating systems and other software regularly with limited data collection and interaction. Microsoft does not need to know *how* consumers use Windows or Office in order to determine whether a user needs a security update; it only needs to be able to detect that a consumer is using outdated software. Occasional communication and inspection is necessary, but the interaction can be scoped in such as a way as to minimally compromise consumer privacy. On the other hand, companies should not be allowed to leverage the need for security updates into an ongoing relationship that involves unrelated data collection, or to shoehorn adware[19] or other

[17] Justin Brookman & G.S. Hans, *Why Collection Matters: Surveillance as a De Facto Privacy Harm*, Future of Privacy F., *available at* http://www.futureofprivacy.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf.

[18] Bruce Schneier, *The Internet of Things is Wildly Insecure – and Often Unpatchable,* WiredOpinion (Jan. 6, 2014, 6:30 AM), http://www.wired.com/opinion/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/.

[19] Ed Bott, *A Close Look at How Oracle Installs Deceptive Software with Java Updates*, ZDNet (Jan. 22, 2013, 11:00 AM), http://www.zdnet.com/a-close-look-at-how-oracle-installs-deceptive-software-with-java-updates-7000010038/.

unrelated data collection functionality onto software shipped for a security update.[20]

2. Deidentification

The FTC has also posed the question whether the Internet of Things poses new challenges for deidentification or aggregation. We do not believe that the proliferation of sensors and internet connectivity necessitates a change to the framework articulated by the Commission in its 2012 report: "as long as (1) a given data set is not reasonably identifiable, (2) the company publicly commits not to re-identify it, and (3) the company requires any downstream users of the data to keep it in de-identified form, that data will fall outside the scope of the framework."[21]

We also urge the FTC to resist interpretations that would weaken that test: the FTC should stress that corporate operational controls to internally mask data that can be readily reversed does not constitute technical deidentification of such data. While operational controls may be an element of a robust deidentification scheme that renders data sufficiently deidentified such that the company could not reassociate the data even if fully motivated to do so, the FTC should reject processes that could be reversed by simple dictionary attacks or association with an escrowed key — even if those activities were prohibited by corporate policy. We believe that there are privacy-preserving benefits to such corporate controls, as well as societal benefits to the longitudinal research that those controls allow. However, calling such data "deidentified" overstates the extent to which that data is severed from personal data.[22] We believe the FTC should retain its technical test that requires that companies reasonably believe that they could not reassociate such data if they so desired.

C. User Control and Accountability

Another troubling trend that has become prevalent in the age of Big Data and the Internet of Things is an effort to substitute corporate accountability for consumer empowerment and choice. Supporters of this view argue that because there are so many devices transmitting so much data about us, consumers cannot reasonably be expected to manage it. We disagree with this new trend toward

[20] Nick Hide, *LG Promises Firmware Update Will Fix Smart TV Privacy Snafu*, CNET UK (Nov. 21, 2013, 5:42 PM), http://crave.cnet.co.uk/televisions/lg-promises-firmware-update-will-fix-smart-tv-privacy-snafu-50012828/.

[21] FEDERAL TRADE COMM'N, *Protecting Consumer Privacy in an Era of Rapid Change* (February 2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[22] See, e.g., Future of Privacy F., *Mobile Location Analytics Code of Conduct*, http://www.futureofprivacy.org/wp-content/uploads/10.22.13-FINAL-MLA-Code.pdf (distinguising "de-personalized" data from "de-identified" data).

data paternalism.[23] Certainly, more sensors and connectivity means that there's more for consumers to control. But the result should be *stronger* and highly *usable* consumer controls, not a reduction thereof.

This is not to say that corporate accountability and privacy by design don't have an important role to play. Companies should have an obligation to make principled decisions about *defaults* and *design decisions* and whether to require an informed opt-in or just to allow an opt-out for data collection (based on, *inter alia*, the sensitivity and comprehensiveness of the data). In some cases, consumer choice may not be appropriate at all — such as where the data collection and use is operationally necessary for product fulfillment, or transactional data that is necessary for fraud prevention. For secondary uses of the data, however, consumers should ultimately be empowered to make decisions about how their data will be collected, used, shared, and retained.

For these reasons, CDT strongly agrees with the recent blog post (and forthcoming white paper) from Dr. Ann Cavoukian, Commissioner Alexander Dix, and Dr. Khaled El Emam entitled "Consent and Personal Control Are Not Things of the Past."[24] The authors note that given widespread attention to expansive corporate and government data collection practices, there is no evidence to support the notion that consumers wished to be deprived of meaningful consumer choice:

> We must also not overlook public sentiment. To argue that the public would readily accept taking away all control of their personal information and giving it to private sector companies and to the government would be a colossal misread of the public's views. There is no evidence that legislators and the public are prepared today to cast aside their existing privacy interests. In fact, there is growing intolerance of data breaches and privacy infractions (with specific reference to unacceptable Big Data pursuits). We need changes that will increase public trust — erosion of personal control will most likely not be one of them.

The design and operation of the Internet are fundamentally predicated upon control *at the ends* — by each end participating in a communication — rather than by intermediaries and other centralized decisionmakers. The Internet of Things should be architected to empower users to make their own decisions, create their own content, and improve their lives in the ways that they see fit. If a consumer pays $2,000 for a smart refrigerator, she should be in control of how

[23] E.g., Eduardo Ustaran, *Yes, Consent is Dead. Further, Continuing to Give it a Central Role is Dangerous.* (Dec. 18, 2013), Privacy Perspectives, https://www.privacyassociation.org/privacy_perspectives/post/yes_consent_is_dead._further_continuing_to_give_it_a_central_role_is_danger.

[24] Ann Cavoukian, Alexander Dix, & Khaled El Emam, *Consent and Personal Control Are Not Things of the Past* (Jan. 8, 2014), Privacy Perspectives, https://www.privacyassociation.org/privacy_perspectives/post/consent_and_personal_control_are_not_things_of_the_past.

information about her use of that refrigerator gets collected and shared. While users cannot be expected to micromanage every decision about how the refrigerator processes and analyzes each item of food that goes in, they need to be able to make general, global decisions about what that device will do with their personal information (as well as other observed information about private places such as the home and office the device is located).

At the end of the day, the consumer should be in control — not the refrigerator.

Finally, as noted above, whether consumer control should be opt-in or opt-out will largely depend on sensitivity and context. However, we also incorporate our previous comments to the Commission on Comprehensive and Platform-Level Data Collection.[25] Intermediaries that a consumer uses to access other services — and that possess the ability to capture cross-service activity — should in most cases obtain a user's informed affirmative consent to collect that data. For this reason, we argued in a recent blog post that LG Smart TVs shouldn't be collecting and sending back to LG information about what consumers are watching without the user's opt-in consent.[26] We urge the FTC to endorse this position.

Possible Methods to Better Enable User Control of IoT Devices and Systems

Given the necessary complexity ushered in by the Internet of Things, we urge the FTC to call on manufacturers to develop powerful, comprehensive controls to make IoT manageable for consumers. Many IoT devices and systems will, by definition, need to communicate through a local wireless network with each other and with other systems in a wider-area network, like the Internet. To get an IoT device up and running on a wireless network, some type of network setup will be required.[27] This network setup step —whether on the device itself or mediated by an IoT networking platform on the local network — is a natural point to interact with the consumer. It is an open question for research and industry if notice about data collection and sharing can be optimized for this interface. Ideally, such interfaces can exploit the user's desire to get a device working on the network to describe the scope of collection and sharing of data such that the user can make well-informed decisions about the use of such products.

[25] CTR. FOR DEMOCRACY & TECH., *Comments of the Center for Democracy and Technology on the Federal Trade Commission's "The Big Picture: Comprehensive Data Collection Online" Workshop* (March 8, 2013), http://www.ftc.gov/sites/default/files/documents/public_comments/2013/03/bigpic-04.pdf.

[26] Justin Brookman, *Eroding Trust: How New Smart TV Lacks Privacy by Design and Transparency* (Nov. 27, 2013), Privacy Perspectives, https://www.privacyassociation.org/privacy_perspectives/post/eroding_trust_how_new_smart_tv_lacks_privacy_by_design_and_transparency.

[27] Note that some types of *ephemeral networking* — like wireless communication involved in Radio Frequency ID (RFID) and Near-Field Communication (NFC) applications — are designed not to require networking configuration.

Standardization of user controls will be important and crucial for a consistent privacy control experience across IoT devices and systems. For example, users may naturally desire the capability to remove all networking functionality from IoT devices for which networked communications is not essential to the purpose of the product. For products that use network access as an added element that may enhance but not be essential to the product's functions, industry might want to standardize physical elements that can disable network communication. This might be as simple as a pull-tab or plastic blister that when removed or broken destroys the antenna or circuitry required for networking. For RFID and NFC-enabled IoT elements, for which there is no persistent networking but only call-and-response data communication, this will be an essential privacy feature. For example, if someone is able to identify the unique identifier in a RFID attached to a milk carton, when that carton is thrown away and carted to a landfill, the same person may be able to identify which bag of garbage came from the target person and use that to examine other sensitive discarded materials.

Configuring an increasing quantity of network-enabled IoT devices could easily become quite daunting. Accordingly, it may be more usable and practical for users to configure IoT privacy controls at the network level. That is, a network-monitoring device could be designed for IoT environments that would allow a homeowner to block or allow certain kinds of communication both within the home and externally to the Internet. For example, a user may naturally want her smart TV to communicate with sources of content outside the home, but might not want it communicating with other devices in the home without explicit permission. As another example, it may be completely inappropriate in the eye of the user for cheap consumer products (e.g. a toothbrush or milk carton) to communicate externally. There is already some standards work being done in the Internet Engineering Task Force (IETF) to provide a trusted agent within a local network that could serve as a single point of service for user controls of IoT device networking.[28] We would like to see industry work to facilitate and develop specific standards for aggregated network-level user control of IoT device and system network communication.

III. Health Applications as a Critical Case Study in IoT

Telehealth technologies — designed to provide medical support and wellness assistance outside of traditional health care settings — will be a critical application of IoT technologies. The benefits of telehealth applications are extensive, beyond simply providing the capability for limited forms of remote medical care and consultation. The prospect for fine-grained, continuous, noninvasive measurements of body signals — blood glucose, heart rate, blood pressure, core body temperature, etc. — that can then be analyzed by expert software systems and health care providers remotely and asynchronously holds enormous potential for lowering health care costs and improving the quality of patient care and wellness.

[28] Phillip Hallam-Baker, *Internet-Draft: OmniBroker Protocol*, Internet Engineering Task Force (July 8, 2013), http://tools.ietf.org/html/draft-hallambaker-omnibroker-06.

However, most telehealth technologies will be provided to consumers by entities that are neither health care providers nor health insurance plans, both of which are covered by HIPAA and subject to HHS enforcement authority. This means there will be little recourse for users that suffer harm or privacy breaches outside FTC Section 5 authority or state law, where applicable. The nature of the data collected — highly sensitive, fine-grained health data —and the prospects for vulnerabilities or flaws in the design and execution of telehealth technologies will mean that the risks of data breach or potential harm to the user will be high. For example, there are serious implications of potential eavesdropping and exfiltration of data off of telehealth devices. If an attacker can cause a telehealth sensor to report a misleading body reading, substantial physical injury or even death may result.

In terms of FIPPs, it is instructive to walk through how each should apply in the critical case of telehealth:

- **Collection limitation/data minimization:** To minimize risks of breach or inappropriate disclosure, telehealth technologies should collect only the body data necessary to perform their functions and should do so at the highest level of granularity (lowest resolution) possible, unless specifically placed in a diagnostic mode by the user or a provider for troubleshooting or calibration. If high-resolution data is needed, it would be best to keep that raw data on the sensing device itself and only transmit aggregate results (averages, medians, min/max, etc.) over the network.

- **Data quality:** It will be especially important that telehealth technologies provide accurate sensor readings, translate those readings into usable medical measurements, and present those readings to the user in a manner that does not result in confusion or adverse medical actions. A failure in any one of these steps could cause the user, or a provider on behalf of the user, to take actions that don't reflect the true state of the body and could cause discomfort, injury, or even death.

- **Purpose specification/use limitation:** Telehealth technologies will have a range of specified purposes to which data will be put to use; some will be narrowly related to reading and storing longitudinal body measurements, while others will have a wider set of functionality, including possibly sharing body readings with a larger community for wellness engagement and encouragement. The range of collection, sharing, and use of data should be crystal clear to the user as close to the first body measurement as possible. Users of telehealth technologies should not receive an unwelcome surprise when readings are inadvertently posted on their social networking profile. Similarly, uses that may not be intuitive at all given the context of health, such as marketing-related uses, should face an even higher bar for user understanding. Only in exceptional cases should non-intuitive uses be made of such data and then only with the explicit, informed consent of the user or as provided by law.

- **Security safeguards:** Data security of telehealth technologies will need to be very carefully considered. Threats to data security include: unauthorized access and modification of data while it is in transit over the network, while the data is resident on the telehealth device or a support device (e.g., a smartphone), as well as access and modification to any software or hardware that make up the telehealth device. Common authentication and encryption methods can substantially mitigate these threats, but security must be a significant focus during the design of the product and the product must be designed to the greatest extent possible to handle emerging threats in the after-market environment and fail safely — i.e., when an error or failure does happen, it should minimize the risks to the user and notify the user in an accessible manner what the error is.

- **Transparency:** Telehealth device and system manufacturers must detail in an accessible manner data practices involved with the devices themselves as well as data practices once the data reaches the manufacturer, if ever. High-level descriptions of practices are acceptable, but it should be possible for more capable users to dig deeper and, for example, learn what encryption standards and authentication methods are being used to protect the device, data on the device, and data in transit from the device.

- **Individual participation:** Users should have access to the data devices record about their bodies and they should be able to easily understand and visualize it. For example, tech-savvy type-I diabetics have complained that they cannot access the blood glucose measurements that are recorded by insulin pumps and then transmitted to the manufacturer. These patients seek to better understand their bodies and feel frustrated and suspicious that the manufacturer wouldn't provide ready access to data that is fundamentally generated by their own body. Openness can help to foster trust in the technology. Patients that chose to examine the data will better understand their conditions as well as the data that is being shared outside the boundaries of their home and body.

- **Accountability:** Finally, the manufacturer of a telehealth technology should have processes in place and staff on hand that can help users negotiate questions and concerns they may have about health data and the interaction with a telehealth device. If companies fail to comply with the above standards, regulators must have the authority to hold them responsible for their failings.

The above sketch of how FIPPs apply to the sensitive-data extreme of telehealth technologies in IoT is useful for thinking about more general IoT applications. While few types of IoT-mediated data will be as sensitive as health data, it can be very difficult to anticipate the risks that IoT devices, systems and platforms will face once deployed in the real world. The more general application of the FIPPs to IoT can be stated quite plainly. IoT technologies should:

- Collect and transmit only that data that is needed for the purpose of the device;
- Make sure data is as accurate as appropriate given potential risks;
- Specify the device's purpose clearly and ensure that subsequent use of the data honor those specified purposes;
- Adequately secure the devices and data against eavesdropping, inappropriate modification, spoofing and other threats;
- Describe in a manner accessible to both the lay user as well as technically-knowledgeable user, data practices and processes both resident in the device as well as after data, if relevant, is transmitted externally;
- Allow the user access to the data recorded and transmitted from the device; and,
- Provide clear mechanisms for users to assess how to accomplish each of the above goals and stipulate redress and support mechanisms for when a user has difficulties or believes some commitment towards this data is not being fulfilled.

IV. Conclusion

We thank the Commission for soliciting additional comments following the successful workshop this past November on privacy and security in the Internet of Things. Despite substantial privacy and security risks inherent in the Internet of Things, we believe FIPPs are as relevant as ever and that the Commission has an important role in terms of guidance and enforcement as the IoT landscape evolves in coming years.

Sincerely,

/s/

Justin Brookman
Director, Consumer Privacy Project; CDT

/s/

Joseph Lorenzo Hall
Chief Technologist; CDT

/s/

G.S. Hans
Ron Plesser Fellow; CDT