WEATHERING THE NEST: PRIVACY IMPLICATIONS OF HOME MONITORING FOR THE AGING AMERICAN POPULATION

JILLISA BRONFMAN[†]

ABSTRACT

The research in this paper will seek to ascertain the extent of personal data entry and collection required to enjoy at least the minimal promised benefits of distributed intelligence and monitoring in the home. Particular attention will be given to the abilities and sensitivities of the population most likely to need these devices, notably the elderly and disabled. The paper will then evaluate whether existing legal limitations on the collection, maintenance, and use of such data are applicable to devices currently in use in the home environment and whether such regulations effectively protect privacy. Finally, given appropriate policy parameters, the paper will offer proposals to effectuate reasonable and practical privacy-protective solutions for developers and consumers.

INTRODUCTION

This article focuses on one subset of the Internet of Things (IoT)[1] revolution, home monitoring technologies. The use of IoT home monitoring technologies especially affects elderly populations using these devices and systems in their homes. The selection of these technologies is not random; in fact, watching the development of these technologies serves as a forecast for the problems inherent in and indicative of future use of similar technologies, the "canary in the

---

[†] Jillisa (Jill) Bronfman, Director of the Privacy and Technology Project at the Institute for Innovation Law at the University of California Hastings College of the Law, Adjunct Professor of Data Privacy Law, and Lecturer in Mobile Communications at San Francisco State University. Jill Bronfman wishes to acknowledge the able assistance of Cassidy Kim, student at the University of California at Hastings College of the Law, review by the Junior Faculty Group at the University of California Hastings College of the Law, and contributions from the Berkeley Privacy Law Scholars Conference.

[1] *Internet of Things*, OXFORD DICTIONARIES, http://www.oxforddictionaries.com/us/definition/american_english/Internet-of-things (last visited Nov. 26, 2015) (defining Internet of Things as the "interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data").

coalmine" for the IoT.[2] Use of IoT home monitoring technologies for the elderly is at this time preliminary as not every household is so equipped. While we may see these devices as necessary and desirable for vulnerable populations, once they become more available, the use of IoT home monitoring devices will become as ubiquitous as other mobile devices. Now is the opportune time to evaluate the privacy implications of these new technologies, before their intrusions become part of the fabric of everyday life.

Further highlighting the importance of these new technologies is the recent Federal Trade Commission (FTC) staff report on IoT, which specifically mentions home monitoring technologies. For example:

> [H]ome automation systems that turn on your front porch light when you leave work; . . . 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 . . . connected smoke detectors and light bulbs.[3]

What are the consequences of collecting this data in the home? The consequences are of three types: (1) the effect on individual behavior and well-being, (2) the effect on corporations and their ability to do business in new and unusual ways,[4] and (3) the effect on

---

[2] FED. TRADE COMM'N, INTERNET OF THINGS WORKSHOP 177, at ll. 12–20 (2013), http://www.ftc.gov/sites/default/files/documents/public_events/Internet-things-privacy-security-connected-world/final_transcript.pdf [hereinafter IOT WORKSHOP] ("[T]here can be amazing benefits, but at the same time, there is a potential for some serious harm, especially in tele-health and health applications. I consider that sort of the canary in the coalmine for the Internet of Things. If bad things start happening with tele-health and health applications, you are going to see that sort of poison the well, so to speak, for a whole lot of additional kinds of connected applications." (Joseph Lorenzo Hall, the chief technologist at the Center for Democracy and Technology (CDT))).

[3] FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 1 (2015), http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-Internet-things-privacy/150127iotrpt.pdf [hereinafter IOT CONNECTED WORLD].

[4] Max Chafkin, *41. SamsungInternet*, FAST COMPANY: MOST INNOVATIVE COMPANIES 2015 (Feb. 9, 2015), http://www.fastcompany.com/3039597/most-innovative-companies-2015/samsung ("'Imagine a world in which these [home] appliances are connected to each other,' says David Eun, a Samsung executive vice president. 'What you'd have is one of the largest platforms for distributing content and services and apps—even ads.' . . . [SmartThings is a] "Silicon Valley startup [that] offers a kit that makes it easy for consumers control

government action. As for the last effect, if the resulting government regulation is unable to protect U.S. consumers, other solutions must be sought.

In evaluating these technologies, we should first consider the benefits to consumers. Home monitoring technologies upgrade the consumer and the consumer's home to a higher standard of living at a low cost. In the case of monitoring elderly and disabled consumers, the cost of a home health care aide may be excessive or prohibitive,[5] relative to purchasing a small device, even with monthly fees. Thus, because just the necessary devices may be purchased, the home monitoring system may be more cost-effective as well as more structurally flexible to scale up and down based on individual needs for assistance. Further, empirical studies have shown that older individuals value home monitoring devices because such devices allow them to age in place, among other reasons.[6]

Next, we should question the amount of private information traded for the use of these new technologies. There is some room for individual variance, but there is also a threshold level of information required for basic participation. Each user must consider how much individual or family information she is willing to upload into the thermostat or medical alert device in order for the device to function optimally. In many cases, the elderly, and particularly the frail or disabled elderly, are willing to downgrade the general expectation of privacy in order to receive the benefits of safety and monitoring technology in the home.[7]

Schlage door locks, GE lightbulbs, Sonos sound systems, and, as a result of the acquisition, all of Samsung's smart appliances.").

[5] Based on 44 hours per week by 52 weeks, the annual estimated cost of a health care aide is $45,760. *Compare Long Term Care Costs Across the United States*, GENWORTH (Feb. 26, 2015), https://www.genworth.com/corporate/about-genworth/industry-expertise/cost-of-care.html (last visited Apr. 27, 2015).

[6] Veerle Claes, et al., *Attitudes and Perceptions of Adults of 60 Years and Older Towards In-Home Monitoring of the Activities of Daily Living with Contactless Sensors: An Explorative Study*, 52 INT'L J. OF NURSING STUDIES 134, 134 (2014) ("[D]escriptive statistics indicate that adults of 60 years and older find contactless monitoring useful for various purposes (e.g. to remain living at home longer, safely and independently; for timely detection of emergency situations and gradually emerging health problems).").

[7] *See* Daphne Townsend, et al., *Privacy Versus Autonomy: A Tradeoff Model for Smart Home Monitoring Technologies*, 33RD ANNUAL INT'L CONFERENCE OF THE IEEE-EMBS 4749, 4749 (2011) ("Older adults are willing to trade privacy (by accepting a monitoring technology), for autonomy. As the information captured by the sensor becomes more intrusive and the infringement on privacy increases, sensors are accepted if the loss in privacy is traded for autonomy. Even video cameras, the most intrusive sensor type were accepted in exchange

When home monitoring technologies are first used, there may be different privacy concerns for different types of collected data. For example, data on the temperature of the home may cause less of a concern than data on insulin levels. Much of existing law revolves around which data is sensitive and which is available for public consumption. For now, there is a heightened sensitivity to video capture and a lesser willingness to trade video for safety, except in the most extreme circumstance – the total obliteration of privacy associated with assisted living.[8]

There will be less of a distinction in sensitivity of information, however, when all of it is combined in a single platform. Indeed, there has been an increasing ability of data processors to capture multiple data points and either enter them into algorithms or combine them into a unified picture of a person. Even seemingly innocuous pieces of information may have economic or strategic value under these circumstances. Combined and cross-referenced data can fit into a mosaic of information that replicates an identity of an individual with increasing ease and accuracy. What we think of as autonomous artificial intelligence may already be in play, and we are creating it ourselves.

Therefore, when we evaluate the exchange of personal data and privacy for convenience and access, we will need to look far beyond the immediate time and place, and even the present-day user. A simple transactional analysis of entering your name, address, or telephone number into a single monitoring device is a limited field of study. We can peer into the future of home monitoring, which has been explored in some detail in science fiction if not legal analysis. Futurists have offered a wealth of analysis, speculation, and science fiction about the dystopian eventuality of autonomous devices that begin to think on their own and operate on their own. In many cases, the scenarios envision a variety of individual electronic elements doing each and both of these activities better, faster, and with more or less humanity than humans. In the most frighteningly imaginative hypotheticals, the information humans have

---

for the height of autonomy which is to remain in the home."). The author's literature review included articles in which seniors were polled on a wide variety of technologies, namely, "[w]earable sensors were predominantly location and physiological monitoring. Environmental sensors included switches, stove temperature sensors, video and infrared cameras, bed occupancy and bed-based heart rate and respiration monitoring. A few focus groups presented implanted physiological and location monitoring chips to participants." *Id.* at 4750.

[8] *See id.* at 4750, 4752 ("Video monitoring has a high loss of privacy and a moderate gain in autonomy hence it is ranked last. . . . Even video cameras, the most intrusive sensor type were accepted in exchange for the height of autonomy remaining in the home.").

fed into the machines results in a collective, conscious intelligence that surpasses what humans can do or control.

In this article, we will focus on the realistic aspects of existing privacy law as applied to home monitoring technologies, to see what works and what falls short. This Introduction has introduced the concept of privacy for the relatively new technologies of home monitoring. Section I will review the existing law as it applies to these technologies. Section II and III will discuss the serious consequences to leaving these technologies occasionally and loosely regulated. Section IV will offer constructive solutions to bridge the gap between unregulated technologies and fully regulated technologies. Lastly, the Conclusion will offer remarks and suggestions for future research.

I. EXISTING PRIVACY LAWS FOR HOME MONITORING DEVICES, SERVICES, AND APPLICATIONS

A. Privacy and Technology, Past and Present

Historically, privacy law in the United States has responded to technologies that non-physically invade the home and its private sphere, seeking to protect the right to be left alone.[9] The privacy right at issue for home monitoring, however, is the right to control access to personal information, and the rights of notice and consent for the distribution of such information.[10] It is the right not to have data extracted from one's private life, and the right to be free from the abuse of your private data

---

[9] *See* Benjamin Wittes, *Databuse: Digital Privacy and the Mosaic,* THE BROOKINGS INST. 8 (Apr. 1, 2011), http://www.brookings.edu/research/papers/2011/04/01-databuse-wittes#_ftnref8 ("The 1890 publication of Samuel Warren's and Louis Brandeis's seminal law review article, 'The Right to Privacy,' and Brandeis's subsequent dissent in the 1928 Supreme Court case of *Olmstead v. United States*—were pivotal in crafting modern American attitudes in law, policy, and culture alike towards the concept of privacy. . . . The Right to Privacy responded to the invention of the instant camera and its use by the press to report on famous people. The Brandeis dissent responded to the development of wiretapping technology."); Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890); Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (taking the continuing stand on the issue).

[10] The FTC articulated these basic principles for online privacy in 2000. *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

by others. This is a concept one scholar has termed "databuse."[11] Thus, we need to move away from legal precedents that consider the home the boundary for personal privacy and toward legal frameworks that reflect the technologies we have, which allow for access to the home and to private information in unprecedented ways.

To access the home and its wealth of private and perhaps valuable data, home monitoring companies are moving into a sacred space. A person's home is her "castle,"[12] and she is the queen of this domain and its primary decision-maker. Historically, "the house of everyone is to him as his castle and fortress, as well for his defense against injury and violence, as for his repose."[13] It is time to consider whether the castle's threshold, both literally/physically and figuratively/legally, can hold back the onslaught of privacy intrusions.

Into the early twenty-first century, privacy in the home has been given significant judicial deference in evaluating whether a Fourth Amendment search and seizure violation has occurred. In *Kyllo v. United States*,[14] the Court held that when the government uses a device that is not in general public use to explore details of a private home that would previously have been unknowable without physical intrusion, the surveillance is a Fourth Amendment "search," and is presumptively unreasonable without a warrant. Note that *Kyllo* turns on the uniqueness of the government's access to high technology. But home monitoring may at some point become ubiquitous. When this occurs, would listening to someone's home monitoring devices be like looking in an open window? Yes, if it is a greenhouse and not the residence per se,[15] but no, if it is inside the house or on the porch. According to Justice Scalia in *Florida v. Jardines*: "When it comes to the Fourth Amendment, the home is first among equals . . . This right would be of little practical value if the state's agents could stand in a home's porch or side garden and trawl for evidence with impunity."[16]

The state's corresponding obligation to respect the home's "well-being, tranquility, and privacy" is an interest "of the highest order in a

---

[11] *See Wittes*, *supra* note 9 ("The relevant concept is not, in my judgment, protecting some elusive positive right of user privacy but, rather, protecting a negative right—a right against the unjustified deployment of user data in a fashion adverse to the user's interests, a right, we might say, against.").

[12] The first legal mention of home equals castle is found in *Semayne's Case*, 77 ENG. REP. 194 (K.B. 1603).

[13] *Id*.

[14] Kyllo v. United States, 533 U.S. 27, 40 (2001).

[15] Florida v. Riley, 488 U.S. 445, 450–51 (1989).

[16] Florida v. Jardines, 133 S.Ct. 1409, 1414 (2013).

free and civilized society."[17] Now uncontroversial, "Supreme Court justices of all stripes today accept that the Fourth Amendment reaches beyond the technology of the eighteenth century and requires application to today's analogous intrusions."[18]

Corporate policies, at least on the surface, reflect this legal precedent. Nest Labs, maker of home automation devices, headlines a section of its privacy policy with "[w]e believe home is a private place."[19] Yet, Nest Labs collects and processes many data points through its devices,[20] with the idea that more data is better.[21] More data may not

---

[17] Jordan C. Budd, *A Fourth Amendment for the Poor Alone: Subconsitutional Status and the Myth of the Inviolate Home,* 85 INDIANA L.J. 355, 401 (2010) (citing Carey v. Brown, 447 U.S. 455, 471 (1980)).

[18] Wittes, *supra* note 9. *See e.g.*, *Kyllo*, 533 U.S. at 40.

[19] *Privacy,* NEST (June 17, 2005) *https://nest.com/privacy/*.

[20] *See Privacy Statement for Nest Products and Services,* NEST (June 17, 2015) https://nest.com/legal/privacy-statement/ [hereinafter *Nest Privacy Statement*] ("What information does the Nest Learning Thermostat collect? The Nest Learning Thermostat collects: Information input during setup, Environmental data from the Nest Learning Thermostat's sensors, Direct temperature adjustments to the device, Heating and cooling usage information, Technical information from the device. . . . *They can also sense whether something in the room is moving*. . . . Nest Protect can do things like detect smoke and CO in your home, and give you alarms and warnings. For example, if Nest Protect sees that smoke or CO levels are rising, it will give you a Heads Up before the danger reaches emergency alarm levels and tell you what the danger is." (emphasis added)); *Privacy Policy for Nest Web Sites,* NEST (June 17, 2015), https://nest.com/legal/privacy-policy-for-nest-web-sites ("If you are logged into your Nest account, we record the IP address you visit our website from, and if you have a Nest device or other connected device, we record adjustments you make to the product through the website interface. We store this data along with your email address, information about your Nest device, data collected directly by the device, a history of your device settings, and any other information we have collected about your use of Nest products and services. See our Privacy Statement for Nest Products and Services to learn more about the usage information collected through our products.").

[21] *See Frequently Asked Questions About Nest Aware with Video History*, NEST (Jun. 18, 2015), https://nest.com/support/article/Frequently-asked-questions-about-Nest-Aware-with-Video-History ("Nest Aware is a paid subscription service that makes your Nest Cam even better with additional features and services. It includes video history, video clips and timelapses, activity zones and improved activity alerts."). The Nest Aware service now saves video for future review with video history subscription with up to 30 days saved for review.

be better, though, if third-party marketing agencies or government entities can access and subpoena that information.[22]

Government entities, however, can access data using less transparent and more direct methodologies than the traditional subpoena. In this vein, the government has been "piggybacking" on more advanced corporate monitoring technologies instead of acting through their own technologies.[23] Police departments use third-party contractors to access a wider variety of surveillance techniques, including cameras, which can monitor public streets, and possibly workplaces and homes.[24] The judicial system must observe this relationship between the government and its corporate subcontractors in its interpretation of the Fourth Amendment and its constitutional companions.

Additionally, the privacy of personal data has historically been protected by relying on contract principles, including the individual's right to notice and the requirement of consent.[25] These rights may falter, however, if sacrificing privacy means the device saving a life. It should be the individual or family, though, who determines how to balance privacy and a device's efficacy.[26]

---

[22] *Cf. Nate* Cardozo, et al., *Who Has Your Back?* Elec. Frontier Found. (May 15, 2014), https://www.eff.org/who-has-your-back-2014 (explaining Nest's parent company, Google, has received six stars, a perfect score, in fighting data requests).

[23] *See Paul* Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1311 (2012) ("As the surveillance society expands, the police will learn to rely more on the products of private surveillance, and will shift their time, energy, and money away from traditional self-help policing, becoming passive consumers rather than active producers of surveillance. Private industry is destined to become the unwitting research and development arm of the FBI. If we continue to interpret the Fourth Amendment as we always have, we will find ourselves not only in a surveillance society, but also in a surveillance state.").

[24] *See* David Sasaki, *SeeChange*, DAVIDSASAKI.NAME (Mar. 3, 2014), http://davidsasaki.name/2014/03/seechange/ ("What did surprise me, what really blew my mind, was the off-handed mention that, in addition to NYPD's own 3,000 cameras, they also had access to 23,000 streaming cameras placed in residential buildings by the private security firm, SecureWatch24.").

[25] *See* Press Release, White House Office of the Press Secretary, We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online (Feb. 23, 2012) https://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights ("[C]onsumers have a right to easily understandable information about privacy and security practices.").

[26] *See* Diane F. Mahoney, et al., *In-home Monitoring of Persons with Dementia: Ethical Guidelines for Technology Research and Development*, 3 ALZHEIMER'S & DEMENTIA 217, 220 (2007) ("Both in the home and in the investigator's

B. Regulation

Who is monitoring these monitors? The IoT industry is largely unregulated, especially when compared to how human in-home health care and 911 services are regulated. Regulations for human in-home care span health and financial concerns, and 911 service technologies are regulated by the FCC.[27] By contrast, while government agencies have monitored portions of the IoT industry, no one agency has been tasked with looking at the ecosystem as a whole to address concerns about security or privacy.[28] As a result of this patchwork regulation, statutory support for consumer privacy in monitoring devices is insufficient. Unfortunately, in order to achieve a fully regulated industry, radical change is needed.[29]

This is largely because any checks on the industry are market-driven. The wide-ranging level of staff training within the industry is a case in point.[30] And while broader health care, financial data, and data

---

laboratory, the gathering, storage, and retrieval of information from such systems must have safeguards built in, to ensure that they meet legal and ethical standards. Research protocols should include specific statements about how privacy and confidentiality considerations will be handled.").

[27] *Home Care Regulatory Issues,* NAT'L ASSOC. FOR HOME CARE & HOSPICE, http://www.nahc.org/advocacy-policy/home-care-regulatory-issues/ (last visited Nov. 26, 2015); Intrado, the primary provider of 911 service, notes on its website that FCC regulations have covered 911, E911, and VoIP technologies. *FCC E911 Legislation*, INTRADO INC., http://www1.911enable.com/resource-center/fcc-e911-legislation (last visited Dec. 27, 2015). The company's products only extend from enterprise to small and medium businesses, but not to consumer use. *See Company Overview*, INTRADO INC., http://www1.911enable.com/about-us/company-overview (last visited Dec. 27, 2015).

[28] *See* IOT WORKSHOP, *supra* note 2, at 184 ("[N]o regulatory agency was looking at the security of these devices. The FCC said, that's not us. The FCC looks at the way the radio transmits, not what is being transmitted. And the FDA said, it's not us. We look at how the medical part of it works. And it turns out that there is this huge gap, that nobody is looking at the security of these devices from a cyber security perspective, from a connected device perspective.").

[29] Scott Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 132 (2014) ("The FTC's standard . . . may mean that in the end all biometric and sensor-based Internet of Things data need to be treated as [Personally Identifiable Information] (PII). That, however, would require a radical re-working of current law and practice." (relying upon FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012)).

[30] *Compare Medical Alert Questions*, LIFESTATION, http://www1.lifestation.com/faq.php#q33top10 (last visited Nov. 26, 2015) ("What kind of training do LifeStation Care Specialists receive? All LifeStation personnel begin their

breach regulations may indirectly touch the industry, those that would have any real effect have not yet passed. Thus, regulation is currently not only lacking in teeth, it also lacks a "mouth."[31]

So much of our privacy landscape has been built upon U.S. squeamishness about revealing healthcare data. We do have the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended and supplemented. The privacy rule for HIPAA "establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically."[32] For home monitoring, the subset of data that is medical data might be regulated under HIPAA. However, HIPAA applies to some medical data collected from consumers but certainly not all. In fact, it skirts much of home monitoring entirely, either because the industry does not collect applicable data or covered providers are not involved in home monitoring.[33] Therefore, if the entity gathering health data is not a

---

education process with formal classroom training followed by mandatory examinations at the end of each module. This period is followed by practical application training under the guidance of CSAA Certified instructors. Following the new hire training process, all personnel are subject to performance reviews on a weekly basis for their first 3 months of service. Thereafter, all reviews are on a quarterly basis.") *with* Kate Rauch, *10 Questions to Ask When Shopping for a Personal Emergency Response System (PERS)*, CARING.COM, https://www.caring.com/checklists/personal-emergency-response-questions (last visited Dec. 27, 2015) ("How is the response center staff trained? There's no government-regulated PERS staff training or certification requirements, so companies train their staff in a variety of ways.").

[31] For example, the Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015 proclaims that, "[i]t is the sense of Congress that each covered entity should provide, when reasonable, a version of the notice required under this Act in a format that is computer-readable . . . ." THE WHITE HOUSE, ADMINISTRATION DISCUSSION DRAFT: CONSUMER PRIVACY BILL OF RIGHTS ACT OF 2015, 1 (proposed Feb. 27, 2015), http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf [hereinafter WHITE HOUSE DRAFT: CONSUMER PRIVACY BILL OF RIGHTS ACT]. In other words, here's an idea, if it's ok with you, you might want to consider doing this. Also, you've got 18 months post-data collection to do whatever you want with the data collected without fear of civil penalties. *Id.* at 18.

[32] *The HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html (last visited Dec. 27, 2015).

[33] IOT WORKSHOP, *supra* note 2, at 179, ll. 16–23 ("And one of the big problems here is a lot of consumer-facing health applications aren't governed by HIPAA.

covered provider like a hospital or medical care provider, there is no protection from HIPAA.

United States privacy law also strongly values the individual and personal nature of financial information. However, the FTC dismisses the Fair Credit Reporting Act (FCRA) as a potential check on the unlimited collection and use of data from IoT devices.[34] The FTC also notes that its own jurisdiction is limited,[35] and calls instead for federal legislation on privacy and security for the IoT. Nevertheless, the FTC promises it will police violations of both "reasonable security" and the FCRA in a limited way.[36]

With regard to users who are both elderly and disabled, the Americans with Disabilities Act (ADA) requires, with some exceptions, that "information obtained regarding the medical condition or history of the applicant is collected and maintained on separate forms and in separate medical files and is treated as a confidential medical record[.]"[37] However, this privacy restriction is limited to the employment context. Employers are the covered entities for the ADA, and while employers are interested in home monitoring of their employees, we still have very few home monitoring devices placed in the home by employers. Regulations for educational institutions and public places also seem like remote connections for home monitoring oversight. Monitoring of employees, students, and the public is an important issue of privacy law, but beyond the scope of this article. Nevertheless, ADA standards may be useful by

---

They are not something provided by a covered entity, they are not a PHR, they are not a personal health record, so they may not have to deal with the breach notification rules. They may at the state level, but not the ones that are now in HIPAA via HITECH." (quoting Joseph Lorenzo Hall of CDT)).

[34] IOT CONNECTED WORLD, *supra* note 3, at 17 ("[T]he 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 then use that data to make in-house credit, insurance, or other eligibility decisions – something that could become increasingly common as the IoT develops.").

[35] *Id.* at viii ("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.").

[36] *Id.* at 53 ("[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.").

[37] Americans with Disabilities Act, 42 U.S.C. § 12112(d)(3)(B) (2012).

analogy when discussing standards for notice and transparency for elderly and disabled users in the solutions section of this article.

Without a coherent federal data breach strategy, the states have stepped in to provide various data breach laws, with varying standards. But no state law addresses home monitoring data or IoT data overall, protects it, or requires IoT data breach notification.[38]

For example, the Children's Online Privacy Protection Act (COPPA),[39] the California erasure law, and other age-based statutes may serve as useful analogies for developing privacy protections for the aging population. But the issues turn on obtaining effective consent from a competent individual, and on protecting data that may be collected from some individuals based on age. COPPA requires that website operators obtain verifiable consent from parents, which is difficult to do because parents are often not the actual users. Similarly, in the context of the elderly who have been adjudicated as legally incompetent, or are functionally unable to give legal consent despite the lack of such adjudication, and are using IoT devices, it would be hard to obtain consent from other family members because it is not their data that is being collected. Matters are somewhat complicated by the fact that the elderly may be legally and financially able to purchase home monitoring devices, unlike children, but may be unable to fully comprehend that data is being collected. Additionally, they may not understand the consequences of collecting that data.

Regulation of home monitoring devices is therefore incomplete at best, pending in several jurisdictions on a more general level but not specific to IoT devices, and desperately in need of a back-up plan to support consumer privacy. At a minimum, if we cannot restrict data collection and use from home monitoring devices—although we should not abandon this effort—we may be able to restrict after-market use of the data for discriminatory purposes. There is a particular need to guard against using data gathered from monitoring devices to discriminate against populations required to use such devices for life-saving measures. Insurers' use of in-home monitoring device data is the most obvious place to begin, which could lead to increased insurance rates based on previously undisclosed or even misinterpreted data, but in nearly all instances is still seen as invasive.[40] Also, IoT data may be subpoenaed in

---

[39] 15 U.S.C. §§ 6501–6506 (2012).

[39] 15 U.S.C. §§ 6501–6506 (2012).

[40] Peppet, *supra* note 29, at 155–56 ("One can easily imagine health and life insurers demanding or seeking access to fitness and health sensor data, or home insurers demanding access to home-monitoring system data. As such data become more detailed, sensitive, and revealing, states might consider prohibiting

cases related to end-of-life and estate decisions made by family members and related life insurance companies. Thus, in order to create an ecosystem of privacy and security for these devices, we will have to look first to the companies themselves.

C. Industry Standards

In the absence of comprehensive regulation, our next hope for protecting consumer privacy would be industry standards. In fact, there has recently been some movement toward industry standards and the establishment of best practices in lieu of government regulation. Industry privacy standards for data security include de-identification of personal data[41] and encryption. The FTC has requested that companies assess and test their security measures as well as minimize the data that they collect,[42] The data minimization standard alone contains several recommendations and concerns. For instance, data can be collected later, or companies can destroy data no longer in use.[43] Although data minimization works in theory, it often fails in practice. For example, a listening TV picks up everything said in the room, not just "turn on TV,"[44] and transmits it to the Internet. Data minimization is thus at odds with the essence of home monitoring IoT, which is constant monitoring and data collection.

---

insurers from conditioning coverage on their revelation . . . Although such information might be useful to a home insurer to investigate a fire or casualty claim, it seems invasive to permit insurers to demand such detailed information as a condition of insurance.").

[41] *But see Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1705 (2010) ("Every successful reidentification, even one that reveals seemingly nonsensitive data like movie ratings, abets future reidentification." (quoting Paul Ohm)).

[42] IOT CONNECTED WORLD, *supra* note 3, at iii ("[C]ompanies 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.").

[43] IOT CONNECTED WORLD, *supra* note 3, at iv ("[S]taff'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.").

[44] Bruce Schneier, *Your TV May Be Watching You*, CNN (Feb. 12, 2015, 9:16 AM), http://www.cnn.com/2015/02/11/opinion/schneier-samsung-tv-listening/ ("We need more explicit conversation about the value of being able to speak freely in our living rooms without our televisions listening, or having e-mail conversations without Google or the government listening. Privacy is a prerequisite for free expression, and losing that would be an enormous blow to our society.").

Nevertheless, data minimization is crucial given this vastness of data collection. When large collections of data aggregate on identifiable platforms or within targetable databases, the danger of breach escalates. Newly-revised data breach laws in California promise notification post-breach, but plans for preventing access and breaches remain elusive. Further, recommendations for data protection regulations in the United States have focused on the collection and storage by large databases.[45] However, smaller providers often collect the information collected by home monitoring devices, and any breaches would slip through the gaps in these regulations. The next section of this article will evaluate what home monitoring device companies are doing to keep their devices and systems secure and the data contained in their systems private.

II. IMPLICATIONS FOR SECURITY

A. Security Ecosystems for Home Monitoring Devices

Data security is a precondition of privacy protection. The FTC met in November 2013 to hear comments on IoT, and issued a staff report in January 2015. The commenters focused on three areas of harm from security breaches of IoT, including personal information, personal safety, and other systems.[46] Thus, companies should consider both physical security, including locked doors and facilities, and network security, including authentication and back-up protocols.

There are exponentially more security issues in a distributed system *vis-à-vis* a centralized system such as a single data center. IoT presents several additional levels of security issues, from the device to the network to the collection or storage of data.[47] This is because the

---

[45] *See* Ohm, *supra* note 23, at 1760; *see also* THE WHITE HOUSE, THE PERSONAL DATA NOTIFICATION & PROTECTION ACT, 2 (proposed Jan. 12, 2015), http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf (addressing data breach notice requirements for "[a]ny business entity engaged in or affecting interstate commerce, that uses, accesses, transmits, stores, disposes of or collects sensitive personally identifiable information about more than 10,000 individuals during any 12-month period").

[46] IOT CONNECTED WORLD, *supra* note 3, at ii ("[P]articipants 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.").

[47] IOT WORKSHOP, *supra* note 2, at 71–72, ll. 11–25, 1–6 ("[A] couple of quick comments on the security issues that are raised by things in the home. I think that you have to worry also about the way that the wireless networking exposes data to interception. We are wary that industries who are moving into this space are not necessarily as mature about the security issues as those as, say, at

security of connecting an IoT device to a home network relies on the security of the home network itself, which may not be secure at all.[48]

What can go wrong when a home network security is breached? First, lax design of security cameras may permit hackers to access live feeds and make them available to the Internet. Cameras, the eyes and often ears of home monitoring, are used to monitor the security of both individuals and property, but may in fact endanger both. The FTC found that the online security cameras made by TRENDnet were easily hacked.[49] The resulting enforcement action against TRENDnet set the standard for future FTC prosecutions of home monitoring networks.

Second, traditional malware, viruses, and worms can infest a home network. Creators of these malware, virus, and worms can either incidentally or specifically target[50] home monitoring devices. A worm, for example, "can be utilized by the attackers to perform distributed denial-of-service (DDoS) attacks."[51] A DDoS attack could wipe out an entire system, leading to shut down of power, light, or other connected systems in the home. Unfortunately, there is not much in the way of financial incentives to build IoT devices with even the most basic security envelopes as the devices are usually inexpensive and unregulated consumer devices. Similarly, there is no financial incentive to upgrade the device with security patches and new versions. Some

---

Microsoft. The relatively cheap or lower grade devices may lack the computing resources or, for economic reasons, there will be less incentive to put good security in them. And fourth, that the security perimeter for IoT devices is actually rather different because, depending on where the endpoint devices are, there may be a higher risk of direct tampering. And there is also a likelihood of multiple or changing environments that IoT devices are expected to operate in, where they will connect promiscuously, don't necessarily have the ability to really know what kind of configuration of what the other device is going to be like." (quoting Lee Tien of the Electronic Frontier Foundation (EFF))).

[48] *Id.* at 101–04, ll. 6–25, 1–15 (quoting Jeff Hagins, the cofounder and chief technology officer at SmartThings, explaining that the security of a whole system of IoT is only as strong as the security of home wifi network, and that there are defects with the widely used WPS wifi encryption technology).

[49] *Id.* at 13, ll. 1–6 ("[I]n the FTC's first enforcement foray into the Internet of Things, we alleged that TRENDnet's lax software design and testing of its IP-connected security cameras enabled a hacker to get his hands on the live feeds from 700 cameras and make them available on the Internet.").

[50] *E.g.,* Dick O'Brien, *The Internet of Things: New Threats Emerge in a Connected World*, SYMANTEC (Jan. 20, 2014), http://www.symantec.com/connect/blogs/internet-things-new-threats-emerge-connected-world ("The attacker was in a position to begin attack[ing] these devices at a time of their choosing.").

[51] *Id.*

older hardware even harbors legacy malware such as the "Misfortune Cookie."[52] In fact, in most cases, there's a counterincentive to make the security open—e.g. allow a back door[53]—in order to allow customer service fixes and upgrades. Many individuals in the security community are familiar with these openings.[54] Regulators have begun to notice the potential consequences of a breach or of publicly available private data being used for unintended purposes.[55]

Finally, the system could simply fail. What happens when the system is breached, data is leaked, or the system simply goes offline? Doors, windows, and locks may open. Temperature controls may cause unsafe low or high temperatures. Any evaluation of the efficacy of a home monitoring system must include breach and failure analysis. A failsafe mechanism, or default protocol, should be built into the system so doors and windows remain secure.[56]

In evaluating home monitoring systems, one must also balance security and safety concerns. In many people's minds, security and safety

---

[52] *See* Robert Vamosi, *Attack of the Home Router,* DARKMATTERS (May 27, 2015), http://darkmatters.norsecorp.com/2015/05/27/attack-of-the-home-router/ ("Last December, US-CERT at the Department of Homeland Security warned broadband router manufacturers of a common vulnerability, dubbed '"Misfortune Cookie."' This vulnerability had actually been patched more than 10 years ago, but was still present on many deployed devices.").

[53] A list of home router models with backdoors was started at https://github.com /elvanderb/TCP-32764/blob/master/README.md (last visited Dec. 27, 2015).

[54] IOT WORKSHOP, *supra* note 2, at 74–75, ll. 18–25, 1–10 ("And so I did a talk this year at a security conference on breaking cameras, like the ones we have in this room. And these devices range from cheap consumer cameras, you know 30 dollars, 50 dollars, up through 1,000 dollar cameras, 1,000 a piece. And I didn't have to do anything special to break into them. They had backdoor accounts left on them. They had simple vulnerabilities that anyone in the security community who looked at it would be able to break. And it doesn't take a lot of technical expertise to do that. And I think the real reason why these exist, why we have these problems in embedded devices is there is no financial incentive to companies to make their devices secure. The example I always throw out is, when is the last time you saw a bad review on Amazon because some product had a security vulnerability? Never." (quoting Craig Heffner, security researcher with Tactical Network Solutions)).

[55] *See id.*, at 12–13, ll. 25, 1–6. Regulatory scrutiny started with the FTC's TRENDnet's investigation but is unlikely to end there.

[56] *Id.* at 348–49, ll. 19–25, 1 ("[A]t that point, the design should take into account what happens when the service does get shut down or when the Internet is unavailable. If the Internet is unavailable, you shouldn't be locked out of your house. Consequently, if the Internet is unavailable, your lock shouldn't fail [to] open, and therefore people would be able to walk into your house." (quoting Marc Rogers, Principal Security Researcher at Lookout, Inc.)).

are synonymous. However, if a home monitoring system contains two-factor authentication to access the system, there is a delay in uploading data to the system, which may decrease the level of safety in, for example, an emergency response system. The risk of security leaks is not just that privacy may be compromised, but that life and limb are in danger. Emergency personnel responding to medical emergencies may be delayed in their arrival at the home.

B. Security in the Home and Homeland Security

Increasingly, security in the home is the foundation for national security. Looking to hack devices connected from people's homes to the Internet? Searches can be performed online,[57] to find networked home devices to hack, and can be done by anyone, including those with commercial or political motives. Access to any one device can allow access to an entire networked system, particularly when the device has no password or security mechanism of its own. When hackers from outside the United States reach home networks, they may find easier access to personal data than they have in the past through the portals established by government entities or large commercial operations in the United States. Therefore, security begins at home, and in the home.

Indeed, there is a pending threat of cyberterrorism against home monitoring systems if national security is dependent on the passwords consumers enter into their home networks. "Passwords are the 'keys to the castle' for important parts of our lives online," yet they are often a weak link in the security of home networks.[58] In addition to data collected by devices connected to the Internet, consumers are voluntarily entering much of the private data collected by the home monitoring devices, including entering their names, addresses, personal contacts, medical information and other personal data in order to sign up for services and activate the devices. One example would be in naming the devices, or the sets of data, including using consumers' and their children's names.[59]

---

[57] *See* SHODAN, http://www.shodan.io (last visited Dec. 27, 2015) ("Shodan is the world's first search engine for Internet-connected devices.").

[58] *See* Joseph Lorenzo Hall, *The Beginning of the End of Passwords,* CENTER FOR DEMOCRACY & TECH. (Oct. 21, 2014), https://cdt.org/blog/the-beginning-of-the-end-of-passwords/ (last visited Dec 27, 2015) ("For something so important, passwords have long been a poor fit: they are frequently stolen in massive quantities, written down on post-it notes attached to the computers they're supposed to protect (please don't do that!), and people choose passwords that are way, way too simple (e.g., "password").").

[59] IOT WORKSHOP, *supra* note 2, at 88–89, ll. 17–25, 1–3 ("[T]he consumers actually add contextual data into the systems. So with our system as an example,

Access to home monitoring devices can have devastating consequences if left available for hacking and other malfeasance.[60] As of 2014, hackers who were able to access Nest Labs devices did so with physical, in-person access to the devices, rather than remotely.[61] But the possibility of remote and system-wide hacking remains, and is perhaps imminent. The potential for cyberterrorism squeaks in at the home-based level in a way few anticipate when they purchase a thermostat or other home monitoring device. Marc Rogers, the Principal Security Researcher at Lookout, Inc., a mobile security company, has speculated that, "a connected thermostat is something of a device that can provide intel of what's going on inside your house, when your house is empty and, if harnessed into a large community of things, can even be used as a weapon to attack critical infrastructure."[62] Homeland security may have stronger passwords, but the federal government may fail to realize its citizens' security is dependent on this fundamental weakness in home security.

Easy access to home monitoring data is not all bad, however. The United States government may want to access home monitoring data to monitor its own citizens to avoid cyberterrorism, and to protect against threats from inside and outside the country. Governments may be interested in accessing the individual data collected by home monitoring devices, transforming it into collective big data, and using it to protect entire cities and states. The use of near real-time analytics of this data go beyond alerting paramedics about individual emergencies, such as a

---

consumers get to group devices by room, for example. And so you can tell at my house, by looking at the data that we have in our system, right, I have my daughters' rooms. And what are they named? My daughters' names, right? Caitlin's room and Claire's room, et cetera, right? And there are motion sensors in those rooms. So access to that data would tell you my childrens' names and whether they are in their room or not. It's very, very private information." (quoting Jeff Hagins of SmartThings)).

[60] *Id.* at 105, ll. 5–16 ("[C]onnected lightbulbs tend to have no security whatsoever, but the connected door lock tends to have more security, right? Because the manufacturer doesn't perceive, and rightly so, that the lightbulb should be secure. And so they put a lot more energy into securing the doorlock than they do the lightbulb. And the question becomes whether that is -- is that an okay thing from a consumer perspective, right, that somebody can drive along in front of my house and hijack my lights, right? Which is completely doable." (quoting Jeff Hagins of SmartThings)).

[61] Lily Hay Newman, *Pretty Much Every Smart Home Device You Can Think of Has Been Hacked*, SLATE (Dec. 30, 2014, 4:38 PM), http://www.slate.com /blogs/future_tense/2014/12/30/the_Internet_of_things_is_a_long_way_from_being_secure.html (listing IoT devices that have been hacked, and how).

[62] IOT WORKSHOP, *supra* note 2, at 304, ll. 17–22.

pending strokes, to alerting city services about group emergencies, such as potential heat stroke due to a power failure.[63]

Nevertheless, government access may be troublesome. As noted by Lee Tien from the Electronic Frontier Foundation, in comments for the FTC IoT workshop in 2013, "[although] we are not discussing government surveillance today, . . . anyone who thinks about the privacy issues thoughtfully, is going to have an eye on what data about household activities or personal activities the government could end up obtaining, either directly from the devices or from IoT providers, whether using legal process or other less savory means."[64]

III. IMPLICATIONS FOR ADVERTISING AND OTHER THIRD-PARTY USES

A. Advertising and Marketing Private Home Monitoring Data

While security issues establish the foundation for consumer privacy, there are several unique privacy issues associated with access to consumer data by home monitoring device companies and their subcontractors. For example, advertising and marketing companies are keen to access personal data in the home in a way previously unimagined. Third-party distribution of home monitoring data is likely to result in targeted advertising by these companies.[65] Connected thermostats tell advertising companies who is home, and when, based on pre-programmed temperatures for the home. This information can be used to send ads, via the home monitoring devices or other media, to consumers in the home.

The most pervasive home monitoring may be in the form of entertainment devices such as televisions. Smart televisions and gaming consoles collect consumer data from the users for the purposes of establishing an account. They also collect data at myriad data points during television viewing and game play. In particular, there are newer, emotive interfaces for voice and gestural input that collect "personal"

---

[63] *See* Erin Bush, *FAQs About Neustar and Our Assistance to Law Enforcement*, NEUSTAR BLOG (July 17, 2012), https://www.neustar.biz/blog/faq-neustar-assistance-law-enforcement (noting the government's longstanding relationship with Neustar, a real-time information analytics company).

[64] IOT WORKSHOP, *supra* note 2, at 68, ll. 10–18.

[65] *Id.* at 364, ll. 9–15 ("Now again, I'm not saying this is happening today, but it would surprise me if we had this entire multi-billion, you know, enumerated Internet of Things and no effort were made for your refrigerator to maybe suggest that you should get some ice cream with the milk that you've just run out of." (quoting Ryan Calo of the University of Washington Law School)).

data beyond that directly entered into the screen.[66] This data can go beyond what the thermostat does to send data about who is home and when. This data will tell advertisers who is lonely, who is hungry, and, of course, who is interested in the shopping channels. The key issue here is that this information may be transmitted to third parties without notice. For example, Cnet noted in February 2015, that "Samsung's Smart TV privacy policy… warns that customers should 'be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition."[67]

In the near future, smart home appliances and monitoring devices will become more like computers. Consumers may view home appliances as designed for the historical purpose, but engineers "view a refrigerator really as a 72 inch computer . . . that just happens to keep your food cold."[68] Each and every connected device captures vast quantities of data, and it is either used by the companies collecting the data, uploaded to the Internet, or both. Video cameras and video capture devices, in particular, collect such significant quantities of data that camera companies are enthusiastic about using the data in new and interesting ways.[69]

---

[66] IOT WORKSHOP, *supra* note 2, at 86, ll. 12–22 ("But these gaming technologies are ushering in a tremendous amount of sensory collection and capture in the living room, right? Between voice commands and machines that are active that are able to listen and detect whether or not particular words are being stated in the room. They contain biometric technology, so they can do some level of face recognition and other kind of avatar recognition for personality. This is, I think, one of the most interesting factors for bringing this kind of connectivity and technology into the home." (quoting Lee Tien of EFF)).

[67] Dan Graziano, *Disable this Feature to Stop Your Samsung Smart TV from Listening to You*, CNET (Feb. 10, 2015, 3:34 PM), http://www.cnet.com/how-to/samsung-smart-tv-spying/.

[68] IOT WORKSHOP, *supra* note 2, at 59, ll. 4–6.

[69] Jared Newman, *The Future of Consumer Tech is About Making You Forget It's There*, FAST COMPANY (Feb. 27, 2015, 6:00 AM), https://www.fastcompany.com/3042948/sector-forecasting/the-future-of-consumer-tech-is-about-making-you-forget-its-there ("'It's really important to not think of video and photo capture as an independent thing to do on the device,' Prober says. 'It's really, "What do you do with the content when it's captured?"' . . . That question will become even more important as new tools like 360-degree cameras become available. Suddenly, you have a lot more footage to work with, which means cameras will need to get smarter at helping you tell the best story." (quoting CJ Prober, GoPro's senior vice president of software and services)).

Granted, smart appliances are alluring. For example, a consumer using these appliances does not need to expend energy ensuring her room remains at a comfortable temperature. Wink, Nest, and Personal Emergency Response Systems (PERS) all rely on this essential transaction: enter some personal data, a little or a lot, very private or not so private, and you will see a fruitful and possibly instantaneous return on your investment. The needle will move on your valuable personal comfort – you will feel the warmth of connection, of safety, or of the air in the room. The smarter a consumer wants the device to be, the more she must feed it with her identity or personal information.

Indeed, the quantity of data created by even a small subset of home monitoring devices connected to the Internet is enormous.[70] To compile the data, at this point there are more devices communicating with the network than individuals communicating with the network, and the number of connected devices is increasing rapidly.[71] The number of devices connected to the Internet has been facilitated by the move from IP v4 to IP v6 and the consequential greater capacity for IP addresses[72] to associate with each device. Further, the ability not only to capture large quantities of data but also to process such data in real time[73] compounds the need to address privacy concerns at this juncture.

---

[70] IOT WORKSHOP, *supra* note 2, at 89, ll. 3–10, 14–22 ("We have less than 10,000 households today, so we are a startup. We just started selling actively at the end of August. Less than 10,000 households using our product, we generate 150 million discrete data points a day out of those 10,000 households. It's an enormous amount of data, most of which would put everybody to sleep . . . Most of the data is not meaningful or useful to anyone, and yet, as I've said, there's a lot of — you can get the entire context of my home. Who is home, what rooms are occupied, the comings and goings of the family. There is an enormous amount of data coming out the house that has to be protected. And certainly I'm at the forefront of this as an industry, but as a consumer, I get very concerned about that data." (quoting Jeff Hagins of SmartThings)).

[71] *Id.* at 7, ll. 10–23 ("Five years ago, for the first time, more things than people connected to the Internet. By 2020, an estimated 90 percent of consumer cars will have some sort of vehicle platform, up from 10 percent today. And it is estimated that, by 2015, there will be 25 billion things hooked up to the Internet. By 2020, we are told the number will rise to 50 billion . . . [including the capacity to] help us remotely monitor an aging family member . . . ."(quoting Edith Ramirez, Chairwoman of the FTC)).

[72] *Id.* at 142, ll. 20–23 ("[I]n February of 2011, we ran out of the IP version 4 32-bit address space, so we standardized in 1996 an IP version 6 128-bit address space." (quoting Vint Cerf, Vice President and Chief Internet Evangelist for Google)).

[73] WHITE HOUSE INTERIM PROGRESS REPORT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 2 (Feb. 2015), https://www.whitehouse.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportun

This increased capacity to transmit data means that more data will be collected and stored from a larger variety of devices. With the increase in the types of data collection devices, this enhanced capacity will result in vast databases filled with personal information. To the extent each new home monitoring technology is added to a platform of connected devices, the incremental creep of additional devices and the barely perceptible change in privacy depletion may not be noticeable or quantifiable. A consumer might say, "I have a television remote and a mobile phone and it is the same technology," generating some enthusiasm for Apple brand iWatches.[74] Watches, in particular, are a familiar mode of technology interaction for older generations of individuals, and may therefore be particularly effective in gently reminding the elderly user to take pills and eat, in addition to serving as an alert device for falls and other in-home emergencies.[75] But the more data available, the more industry will step up to use this data for positive aspects (individual and collective safety), negative ones (surveillance, hacking), and uses that can go either way (hyper-targeted marketing, insurance design).

Home monitoring data may indeed be used for positive social purposes. Initially, advertisers could collect home monitoring data related to door locks to see who might be interested in insurance or alarm systems. Then neighborhood watch organizations could use individual home monitoring data collected by marketing databases for alerts. Additionally, the FTC touts the wonderful benefits to energy conservation if, "[i]n 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,' thus empowering

---

ities_Preserving_Values_Memo.pdf ("[D]ata analysis is increasingly conducted in speeds approaching real time.").

[74] John Melloy, *Apple May Sell 1 Billion 'Life-Saving' Watches*, CNBC (Mar. 9, 2015, 1:31 PM), http://www.cnbc.com/id/102488957?__source=xfinity|mod&par=xfinity (Explaining that during the final stages of the initial draft of this paper, Apple released the Apple iWatch, widely touted as a "life saving device."). Query whether wearable self-monitoring devices will replace home monitoring systems entirely or merely interact with them.

[75] *Lively 24/7 Emergency Medical Alert System,* LIVE!Y, http://www.mylively.com/how-it-works (last visited Dec. 27, 2015) ("Simply plug the Lively hub into a power outlet—it just starts working. Then place activity sensors around the home, activate the account online and start wearing the watch. No home Internet connection or phone line is required. It's that simple . . . The clip and monthly auto fall-detection monitoring service will be available in late 2015 for a nominal additional charge.").

consumers to 'make better decisions about how they use electricity."[76] Comparative data is used to show whether one's home is using more or less electricity than the neighborhood or city average.

But it doesn't take a vivid imagination to wonder what other data may be shared with the neighbors. IoT devices collect a much greater quality and quantity of data; a standard model of notice and consent for use may not be able to encompass the potential uses and misuses of this data.[77]

B. Notice and Consent for Marketing Use

Standard notice and consent requirements are over-inclusive in the sense that they ask for notice and consent where the consumer may not necessarily be interested. For example, a home monitoring consumer may only use the camera function for video, but not audio. As a result of the lengthy and possibly irrelevant language in privacy policies, few consumers read notices and fewer read them thoroughly.

More importantly, the policies may also be under-inclusive in the sense that they notify consumers that data will be collected without fully fleshing out the *types* of data that will be collected, or how the data will be used.[78] Familiar technologies, such as a camera, may be used to collect data in unfamiliar ways. Nest's Dropcam camera collects environmental data as follows: "We collect data from several sensors built into Nest Cam. These sensors collect data such as camera temperature and ambient light in the room. By recording this information, Nest Cam can know, for instance, whether it's dark and it should turn on night vision . . . . We may process information from your camera so that we can send you alerts when something happens."[79] This is arguably beyond a camera's obvious purpose of simply recording what it sees, and may lead to a host of "surprise" uses of the data yet to be imagined.

The way information is gathered on devices present additional challenges to the notice and consent model. The information is provided as a continuous flow rather than provided in bursts of information or with

---

[76] IOT CONNECTED WORLD, *supra* note 3, at 8 (citations omitted).
[77] *See* Section III.C *infra* for further discussion of imaginable misuses.
[78] IOT WORKSHOP, *supra* note 2, at 322, ll. 14-22 ("The other thing is also to make sure the consumer understands what data is being collected. It's one thing to say that data is being collected, but it's another thing to say that actually we are collecting your telephone number, we are collecting your birthdate, we are collecting your sex. You have to be very clear about it so that they can understand what the implications of that data being shared are." (quoting Marc Rogers of Lookout, Inc.)).
[79] *Nest Privacy Statement*, *supra* note 20.

a digital transmission by the consumer.[80] When this information is provided continuously, there are fewer opportunities for user interface and input, and therefore fewer opportunities to interact with the consumers and obtain consent for use of their data. Small consumer devices such as smart light bulbs may have no screens for user interface. Devices may be updated by the system automatically without user notice and consent. The window of opportunity for notice and consent may be lost for short-term use of disposable products that create a long trail of data and fill the databases with personal information.

There's a significant logistical effort involved in notices for home monitoring devices as well. Notice has at least two triggers in the home monitoring application. One, can any reasonably simple and understandable notice cover what the data is actually used for?[81] And two, how do we provide notice when there's no user interface on the device?[82] The FTC is aware of this issue and cautions, "[s]taff 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."[83] Particular attention will be needed

---

[80] IOT WORKSHOP, *supra* note 2, at 123, ll. 6–13 ("This notion of continuous monitoring, which came up very briefly in the panel discussion, is important for several reasons, not the least of which that continuously monitoring things tells you about the processes in a much more refined way then if you showed up at the doctor once every six months or once every three months or only when you're sick." (quoting Vint Cerf of Google)).

[81] *Id.* at 98–99, ll. 21–25, 1–8 ("Whereas there are so many examples today of cases where information is getting shared, like how many people have pushed the button to say "okay" on a notice from your phone that says such-and-such application wants access to your location. And you say, okay. Well, what's it doing with that information, right? And does it mean that the phone is just accessing the location, that the application is only accessing the location local to the phone or is it accessing that location information and shipping it off somewhere? And the answer is, you don't know. But you've said okay." (quoting Jeff Hagins of SmartThings)).

[82] *Id.* at 99, ll. 12–25 ("And that's assuming, you know, that the device even has any kind of an interface for the user, right? Many of the devices -- I think many of the devices we would be looking at, especially with smaller ones, I mean, we already have display problems even with the machine that is designed to show you all sorts of things. The idea that anyone would -- you can't do 80 screens, it doesn't make sense. And if it is an alarm clock, that is not actually going to be providing any sort of direct notice. You know, the entire sort of notice and choice aspect of Fair Information Practices has a real breakdown with a lot of these kinds of built-in devices." (quoting Lee Tien of EFF)).

[83] IOT CONNECTED WORLD, *supra* note 3, at v.

to address the needs of the older populations in their willingness to use certain technologies for notice and consent, and ADA-like access for elderly disabled consumers should be embedded in each of these possible alternatives to text notices. Additionally, user interface notice and consent procedures may have to be re-formulated to encompass notice on multiple platforms: app, device, smartphone, console, laptop, etc.

Not all privacy policies and terms of use address third party use of information. If they do, the terms of the notice and consent may be broad enough to encompass some rather socially abhorrent practices. As a consequence, marketers may make use of personal data as described herein, and without restriction. In addition, there is the specter of concern about use of third party data for insurance purposes. Insurers would be eager to gather personal data in the home either ostensibly by an insurer providing the device and collecting the data, or by the insurer "piggybacking" on existing data. In addition to concerns about blacklisting certain customers, or redlining certain neighborhoods, the insurer might make the disclosure of such data a precondition to obtaining insurance or obtaining a lower rate for existing service.[84] In early 2015, an insurer offered customers exactly that deal.[85] It is difficult, given the United States legal framework of contract law inclusive of notice and consent, to argue that these uses of personal data are "illegal" or beyond the scope of the implied contract. Assuming notice was given properly and consent was obtained within the context of U.S. contract law, the use has been considered fair.

Consumers, especially older or burdened consumers, may want to read a privacy notice for a single device or website, or perhaps even a few, but when home monitoring devices become embedded in nearly every household appliance, consumers are unlikely to read and consent effectively to each privacy notice. Furthermore, home monitoring presents different challenges for notice of collection for able-bodied individuals and for senior/disabled product offerings. In order to calculate a cost-benefit ratio for consent for the adoption of IoT devices in the home, society must look at the benefits of such devices. One of the

---

[84] IOT WORKSHOP, *supra* note 2, at 211, ll. 14–22 ("[Y]ou could start to see a home insurer, for example -- I mean, I love the General Electric example this morning of leaving your -- you know, your stove telling you you are leaving your stove on. Well, I'm pretty sure my home insurer would love to know that, if I was routinely doing that. Could they, as a condition of my insurance, require me to have my appliances share that information with them?" (quoting Scott Peppet, a professor at the University of Colorado Law School)).

[85] Jose Pagliery, *Would You Wear a Tracker to Get an Insurance Discount?*, CNN (Apr. 8, 2015, 5:23 PM), http://money.cnn.com/2015/04/08/technology/security/insurance-data-tracking/.

primary benefits is automation of data collection and upload, i.e. that the consumer does not need to manually transmit the information.

The differentials for consent include impaired consent or family consent for patient, authentication and identification problems, and data retention lifespan issues. How can we ascertain notice and consent for an elderly patient on the Alzheimer's spectrum or in the early stages of dementia? Obtaining effective consent from an elderly patient would fall under the auspices of elder law rather than privacy law, once notice is given. If someone other than the user has purchased a system for a disabled patient, who is the user for authentication and access purposes? Likewise, the notice might have to switch from the data collection subject to the purchaser/user depending on the capacity to consent issues raised by elder law and disability law. Data retention presents a somewhat lesser burden for the elderly than for students, who are fully in possession of many of the rights and responsibilities of adults but have also the right to be forgotten under erasure laws for those under 18 years old.

The FTC has tried to minimize the burden of endless notices by limiting them to unexpected uses, with the following guidance: "For uses that would be inconsistent with the context of the interaction (i.e., unexpected), companies should offer clear and conspicuous choices."[86] Conversely, the latest bill proposed by the current administration proposes that if the use is exactly what the customer asked for, companies may presume notice and consent.[87]

C. Imagined Harms for Unimagined Uses

IoT home monitoring devices designed to save lives or at least improve comfort may collect data beyond what is necessary to provide the service. As the technology expands beyond use by the elderly and disabled users to the broader population, this very personal in-home collection of data may be used for financial gain by third parties.

There are concerns that only rich individuals and families will benefit from home monitoring. Perhaps, conversely, the poor may be monitored more intensely, either through "voluntary" economic incentives or individual necessity.[88] There is very little regulatory

---

[86] *Id.* at vi.

[87] WHITE HOUSE DRAFT: CONSUMER PRIVACY BILL OF RIGHTS ACT, *supra* note 31, at 8 ("Personal data processing that fulfills an individual's request shall be presumed to be reasonable in light of context.").

[88] IOT WORKSHOP, *supra* note 2, at 212, ll. 8–12 ("I'm not sure this is really a problem of an economic divide, like the poor aren't going to be able to get enough sensors. I think the poor are likely to have sensors imposed on them, far

prohibition of economic discrimination based on the collection of data through home monitoring devices, as long as it is accurate.[89] Although elderly and disabled users may, in theory, fall on either side of this economic spectrum, they should be considered among those particularly vulnerable to unimagined uses of their data. The elderly are vulnerable because of their unfamiliarity with new technologies, and the disabled are vulnerable because of their difficulty in using the technologies. These concerns are amplified by the necessity of these technologies in the lives of both the elderly and disabled.

A new bill proposes to address this issue of "disparate impact" resulting from data analysis and targeted use.[90] It remains to be seen, however, whether simply raising or even proscribing this issue will eliminate this sort of data analysis. There are "black box" algorithms, designated trade secrets by the data analysis and advertising companies, which protect advertisers' rights to withhold information needed to correctly police this issue.[91]

It may be premature to declare an absolute harm from unimagined uses. Perhaps consumers would like to be delighted and surprised by new uses and see them as improvements to the quality of their lives. How should we measure this and obtain informed consent? A "surprise me" check box option would capture the high-risk tolerance population, but without further specification, few would choose this

---

more than everybody else." (quoting Scott Peppet of University of Colorado Law School)).

[89] Peppet, *supra* note 29, at 128 ("[T]he FCRA is designed to ensure *accuracy* in credit reports . . . Accuracy, however, is really not the problem with Internet of Things sensor data. One's Fitbit, driving, or smart home sensor data are inherently accurate—there is little to challenge. What is more questionable are the inferences *drawn* from such data . . . Thus, the FCRA provides consumers with little remedy if Internet of Things data were to be incorporated into credit-reporting processes.").

[90] WHITE HOUSE DRAFT: CONSUMER PRIVACY BILL OF RIGHTS ACT, *supra* note 31, at 9 ("Disparate Impact.—When analyzing personal data in a manner that is not reasonable in light of context and results in adverse actions concerning multiple individuals, a covered entity shall—Conduct a disparate impact analysis to determine whether the analysis of personal data described in subsection (d) results in a disparate impact on individuals on the basis of age, race, color, religion, sex, sexual orientation, gender identity, disability, or national origin.").

[91] *Our Data, Our Rules?,* THE BRIAN LEHRER SHOW (Jan. 6, 2015), http://www.wnyc.org/story/our-data-our-rules/ (last visited Dec. 27, 2015) (Frank Pasquale, professor of law at U. Maryland, discussing his book, *Blackbox Society: The Secret Algorithms that Control Money and Information*, available at http://www.hup.harvard.edu/catalog.php?isbn=9780674368279).

option. A company could offer proposed future uses in the notice, but these may not be sufficiently definite to be construed as legally-enforceable contracts. So far, privacy notices have not been held to a contract standard.[92] Further, devices with multiple sensors in the home can be combined to create new and highly intricate portraits of individuals.[93] In that sense, nearly every use is a surprise, or an unintended use, because it can be combined with other data and/or transferred to third parties via bankruptcy, merger, or acquisition.

Yet again, the collection and analysis of data may have a positive effect on the individual generating the data. For example, normalization of the individual's data may occur. This happens when data is streamlined to yield a "normal" value representing the individual's comfort zone, used by the system as a default. The effect will be immediate when an aberrant temperature in the home creates an alert that causes the home's resident to change or normalize the temperature, either through manual adjustment or through a preset, programmed response.

Privacy is always an individual calculation. Privacy is still important to older users of home monitoring devices, but the calculation may result in a different decision. For elderly users, the ability to be identified and located is an important value if the purpose is to get immediate attention. Individually worn healthcare devices can identify individuals with great certainty.[94] Wearable devices are luxurious rather than necessary for functioning in society, unless they are fall alerts connected to a home monitoring service, which become nearly a necessity for a fragile, elderly individual. In the future, geo-location and identification devices may become functionally or literally invaluable as they become the foundation for receiving emergency medical care. Vulnerable consumers may welcome this development, or may choose

---

[92] *See* Dyer v. Northwest Airlines Corp., 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004)*;* Daniel Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUMBIA L. REV. 583, 595–97 (2014) (finding that privacy policies, unlike terms-of-use documents, are typically perceived as non-contractual in nature).

[93] Peppet, *supra* note 29, at 93 (citation omitted) ("Just as two eyes generate depth of field that neither eye alone can perceive, two Internet of Things sensors may reveal unexpected inferences. For example, a fitness monitor's separate measurements of heart rate and respiration can in combination reveal not only a user's exercise routine, but also cocaine, heroin, tobacco, and alcohol use, each of which produces unique biometric signatures. Sensor fusion means that on the Internet of Things, 'every thing may reveal everything.'").

[94] IOT WORKSHOP, *supra* note 2, at 170–71, ll. 24–25, 1–2 ("Ira Hunt, who is the CIO of the CIA said you can be 100 percent identified, as an individual, by your Fitbit data. Why? Because no two persons' gaits or ways of moving are the same." (quoting Scott Peppet of University of Colorado Law School)).

lower-tech options that may be more expensive and/or less supportive of their needs in order to protect their privacy in a largely unregulated field.

In fact, consumers may not be fully aware of privacy and security flaws or be able to fix them even if their awareness of such issues is fully developed.[95] The FTC, and indeed the entire U.S. government, takes a stance on the issue of privacy and security that relies on the assumption that educating the consumer will solve every flaw in the system. The solution may be to make consumers aware of the issue, but also to rely on developers to close the security gaps.[96] Developers can close the gaps by adding privacy by design methodologies to product design. The following section evaluates the efficacy of this hybrid solution.

IV. POTENTIAL PRIVACY SOLUTIONS FOR HOME MONITORING DEVICES, SERVICES, AND APPLICATIONS

A. Waiting for Developer Knights in Shining Armor

Developers have the ability to take constructive action before products hit the market to prevent privacy violations and security breaches. The process begins with quality assurance principles and security by design. Security is a necessary precondition to privacy, and it can be baked into home monitoring devices. There is value in preconditioning home monitoring appliances to prevent both use outside of acceptable parameters for the device and hacking.[97] Technical

---

[95] *Id.* at 77, ll. 4–17 ("Unfortunately, I don't think that trying to educate users will get us where we need to be. You know, the mantra for years in computer security has been educate the user, educate the user. Well, guess what? We've had security problems for decades. That clearly isn't working. Users don't understand the technologies they are dealing with. I hear the term, people always say, people are so technologically — you know, they understand all this technology. No, they don't. They have a phone with pictures on it and they point at the pictures. That is not understanding technology. My 1-year-old can unlock my phone. She has no idea what technology even means." (quoting Craig Heffner of Tactical Network Solutions)).

[96] *Id.* at 77, ll. 18–21 ("So I think we really need to push vendors towards security as these embedded systems come out and become more prevalent and, in reality, they already are." (quoting Craig Heffner of Tactical Network Solutions)).

[97] *Id.* at 106, ll. 10–17 ("So you can't set your range to 1,000 degrees. Somebody can't set your refrigerator to 90 degrees and have all your food go bad and the milk spoil. They only work within reasonable parameters that a consumer might use the product for. So you can build that software into the devices themselves, which further adds to the security and the safety in the system." (quoting Mike Beyerle of GE Appliances)).

standards for secure design are available online and updated frequently.[98] As a foundational matter, universities must educate developers to design products that are not only beautiful and clever, but also secure.[99] Companies should also hire engineers with security knowledge and experience (not just generic software developers) to design and maintain these programs.

In theory, consumers would only buy secure products that will protect their privacy. In reality, market information on this subject is scant and unreliable. Worse yet, there will always be certain consumers who choose to buy less secure devices because they prefer cheaper or trendier products. Therefore, designers of secure IoT solutions for the home should evaluate the scalability of solutions up to network level and down to consumer level. While securing data privacy may not be at the forefront of a device engineer's concerns,[100] it should at least be on her checklist.

For consumer-friendly options, designers and developers could look to ADA standards for access to digital media, including mobile devices. Microsoft has taken the initiative in this regard by not only creating accessible options baked into its offerings, but also developing instructional videos explaining how to use these options and posting them on YouTube.[101] Both developers and consumers can access and use accessibility options to allow users with sensory disabilities to effectively use the service. In the case of IoT devices, notices for privacy may lean on these for platforms that support IoT devices, or use these methodologies as guidance for direct device use.

---

[98] *See Standards for M2M and the Internet of Things, Published Specifications,* ONEM2M, http://www.onem2m.org/technical/published-documents (last visited Mar. 9, 2015).

[99] *See e.g., MSIT in Privacy Engineering*, CARNEGIE MELLON UNIVERSITY, http://privacy.cs.cmu.edu/ (introducing Carnegie Mellon's Master of Science in Information Technology – Privacy Engineering program).

[100] Cliff Ortmeyer, *IoT Privacy: Engineering Fault, Not User Issue*, EBN (Apr. 23, 2015), http://www.ebnonline.com/author.asp?section_id=3507&doc_id=277329&page_number=1 ("Between the development of IoT standards, the selection of wireless technologies, and the adoption of an appropriate Internet Protocol, most engineers are still wrapped up in the basic infrastructure of IoT. As a result, more abstract ideas such as personal privacy can quickly fall by the wayside.").

[101] *See* Microsoft, *Quick Tutorials*, YOUTUBE, https://www.youtube.com/playlist?list=PLtSVUgxIo6KoI5ogCBZuAjB6HprjiaKNM (last updated Feb. 6, 2015).

B. Personal Protection and Decision-Making

Individual activities and precautions may be the final frontier for home network security. Developers can implement privacy and security by design. Companies can offer privacy-protective products and services. Ultimately, the future of privacy and security will depend on consumers paying attention to and paying for privacy. Consumers will learn to pay more for products where privacy protections will have been incorporated into their products by design. On their end, consumers must look beyond password entry. The security levels of network password protocols have been covered at length, and are beyond the scope of this article. In this article, a home-based solution is explained.

Generally, home monitoring devices are on the lax end of the security spectrum *vis-à-vis* commercially-networked devices, as the latter can rely on platform-based security solutions. This lack of baked-in security and privacy controls leaves consumers, by default, in charge of their own security. Consumers are not helpless to defend themselves against privacy intrusions, but they must take action.

Consumers can input effective password protection, if the feature is available on the home monitoring device. If they have password thresholds at all, then there is a need to notify or even require customers to re-set default passwords. For newer devices, consumers may be able to use biometric or other alternatives to passwords, such as encryption for uploaded video feeds[102] and other protection of data in transit to ramp up privacy protections.

Consumers can limit the amount of data entered into the device, a sort of data minimization on the ground level. Also, consumers can take action to delete their data on any given system, assuming it has not been shared pursuant to the consent or other exceptions listed on the privacy policy for that device.[103] Indeed, consumers of IoT equipment

---

[102] Klint Finley, *Stalk Yourself at Home with this Free App*, WIRED (Mar. 16, 2015, 8:00 AM), http://www.wired.com/2015/03/app-lets-stalk-home/ ("It's hard not to worry about uploading video footage from your house to the cloud, but Maslan says that all the video is encrypted so that not even Camio's engineers can access it (though it's not possible to verify this without auditing Camio's servers). For people uploading video that's not particularly sensitive – such as publicly viewable areas such as their front yards — this might not be a big deal. Everyone else will need to take a leap of faith.").

[103] *Nest Privacy Statement*, *supra* note 20 ("You can delete the information on the Nest device by resetting it to the defaults (using Reset in the Settings menu). You can access, amend or delete your personal information from Nest's servers through the controls in your account. Because of the way we maintain certain Services, after your information is deleted, backup copies may linger for some

can interconnect their devices to a secure platform, or at least a secure home network.[104] Even these simple steps, however, may be onerous for the oldest users, and baked-in privacy by design and security by design are superior offerings.

There may be technical solutions that can be implemented on the home network level by individual consumers. This could be done through add-on products that protect a set of home monitoring devices as a wider system.[105] At least one company offers such a service.[106] Such platforms that manage home security and monitoring systems are proliferating, offering users additional choices to make simpler choices in the future with regard to privacy notices. Privacy controls could be done once for the platform rather than for each standalone device. Ideally, privacy notices will offer users a choice to revoke or revise their privacy level elections as their understanding or situation changes.

The most significant downside to platform-based home monitoring controls is that the platform, which houses all the aggregated data, provides a single point of entry for hackers. Even if that point is more secure than each of the standalone devices, hackers may still be successful. Also, there are limitations on a platform-level security barrier, including the ability of applications to collect data outside

---

time before they are deleted, and we may retain certain data for a longer period of time if we are required to do so for legal reasons.").

[104] *See How to Secure Your Wireless Home Network*, WIKIHOW, http://www.wikihow.com/Secure-Your-Wireless-Home-Network (last visited Dec. 27, 2015) (Noting that simple instructions are available online for making a home network more secure.).

[105] IOT WORKSHOP, *supra* note 2, at 216–17, ll. 12–25, 1 ("Something that I would like to see exist is something I put on my home network before my cable router, DSL modem, or whatever, that allows me, in bulk, to anoint certain kinds of data that flows forth from my house. So that's a way of sort of aggregating consent-like stuff. It sounds a lot like DuoTrack, it sounds like other things like ad identifiers and things like that. And you would need some basic standard so that telehealth companies that do anything related to the Internet of Things could mark certain packets as, here's the thing, here's what it is trying to do, so that you could then preclude certain data from flowing forward. It's not a perfect solution, but it might help." (quoting Joseph Lorenzo Hall of CDT)).

[106] *Bitdefender BOX*, BITDEFENDER, http://www.bitdefender.com/box/ (last visited Dec. 27, 2015) ("Advanced Threat Protection: Not just for your computers. Everything. Once connected to the Internet, every device, even Smart TVs, smart appliances like fridges, thermostats or gaming consoles are vulnerable to malware that silently does its work. BOX protects everything else that's in the home: PCs, Macs, Android and iOS tablets and phones alike. Just like an antivirus for your home network.").

platform parameters and the need to pre-identify known threats.[107] Data anonymization, meaning masking the personally-identifying aspects of data, has some utility but in reality it reduces functionality when the purpose of this data is to identify, locate, and potentially save the life of an individual user. Data minimization is an underutilized technique. Applying "just in time" saving strategies from manufacturing to data privacy principles would result in a "just enough data" to do the job. Data beyond the requisite amount needed for functionality should not be collected, analyzed, and/or stored.

C. Expansion of Existing Regulations to Cover Data Gathered by Home Monitoring Devices

HIPAA provides a model to evaluate future regulation of home monitoring in some cases. HIPAA regulation was expanded in 2013 to include the Business Associate (BA) agreement requirement, aiming to encompass business associates who contract with covered entities.[108] In the transcript of the FTC workshop on IoT, Lee Tien of EFF noted that, for a California proposal, "[w]e also use rules that are modeled after HIPAA business associate type rules, so that downstream recipients of data shared from the utilities are bound in a similar way."[109]

HIPAA could be expanded again to include under its regulatory umbrella any business that captures, processes, and stores health data. Under this scenario, medically significant, extremely private data will have some protection. Just as HIPAA was expanded in 2013 in response to concerns about new technology for accessing data via additional systems, it could be expanded incrementally over the next few years to encompass personal health data emanating from home monitoring devices collecting information.

---

[107] Molly Wood, *CES: Security Risks from the Smart Home*, N.Y. TIMES (Jan. 7, 2015), http://www.nytimes.com/2015/01/08/technology/personaltech/ces-security-risks-from-the-smart-home.html?mwrsm=Email&_r=1 ("But as with most antivirus and anti-malware products, the box can scan for and detect only code that has already been identified as a threat. Something new could still sneak through. And the box can't do anything about the personal data harvested by all the various apps that control smart devices in the home or outside of it.").

[108] The HIPAA Privacy and Security Rules regulated health care providers, health plans and companies that process health insurance claims. Revisions to the original rules added business associates of these companies that have access to protected health information, including the covered entities' contractors and subcontractors. http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html.

[109] IOT WORKSHOP, *supra* note 2, at 70, ll. 4–7.

The expansion of HIPAA still leaves the routine data of climate, location, and home occupant data unprotected. To that end, the staff of the FTC would like Congress to go beyond mere security breach notifications, which they believe would better protect the security of data and thereby allow health care monitoring and support devices to function properly.[110]

Pending federal bills would create a coherent scheme for protecting data and establishing breach notifications. For example a proposal from the White House suggests that covered entities for privacy protections be expanded to cover any "person that collects, creates, processes, retains, uses, or discloses personal data in or affecting interstate commerce,"[111] a much broader standard that could include home monitoring devices and platforms. Enforcement capabilities under the White House proposal would rest with the FTC under its traditional authority to protect consumers.[112] The bills reflect a trend towards broader responsibility for data collection, processing, and storage. This would address the current issue of possible home monitoring privacy legislation being too specific. Even IoT privacy legislation may be too specific to gain broad-based political support.[113]

CONCLUSION

Now is the time to evaluate potential home monitoring regulation and its alternatives. But while we wait for pending developments at the federal level on consumer privacy and data security, consumers can make market choices and personal choices with their data that serves to protect them. At this point, consumers have begun to weigh the options presented to them in the world of IoT, and its entry into their homes. They should continue to make informed choices about their privacy before a breach occurs. To begin, some people might opt out of using home monitoring devices. These individuals might prefer to incur

---

[110] IOT CONNECTED WORLD, *supra* note 4, at vii–viii ("General data security legislation should protect against unauthorized access to both personal information and device functionality itself. 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.").

[111] WHITE HOUSE DRAFT: CONSUMER PRIVACY BILL OF RIGHTS ACT, *supra* note 44, at 1.

[112] *Id.* ("A violation of Title I of this Act shall be treated as an unfair or deceptive act or practice in violation of section 5 of the Federal Trade Commission Act (15 U.S.C. § 45).").

[113] *Id*. at vii ("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.").

the more expensive cost of human care and monitoring. Some others may choose less invasive devices that gather information but do not transmit the information to the Internet.[114] Others still may use commercially-available or home-grown privacy protection devices that layer security and privacy on top of home monitoring devices.

This is a transitional moment in the adoption timeline of home monitoring technologies. In order to decide how much security and privacy these devices need, we have to decide as a society where home monitoring devices fit on the scale of importance, from equivalent to national security or to the lesser standard of disposable and recreational gadgets. TRUSTe, an online privacy management service, noted that 22% of consumers believe that the benefits of IoT devices outweigh the risks to privacy.[115] At this point, it is safe to assume that these devices will be a part of home life for many of us. We must therefore act accordingly to secure home monitoring systems from hacking and unauthorized data collection.

[114] The author of this paper has a non-IoT pedometer. Occasionally, the author wears it.

[115] *TRUSTe Privacy Index: 2014 Internet of Things Edition*, TRUSTE (2014), http://www.truste.com/resources/privacy-research/us-Internet-of-things-index-2014/ (last visited Dec. 27, 2015).