Weathering the Nest:
Privacy Implications of Home Monitoring for the Aging American Population

(forthcoming in
Duke Law and Technology Review)

Jillisa (Jill) Bronfman, Program 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 (UC Hastings), 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.

Paper Title: Weathering the Nest: Privacy Implications of Home Monitoring for the Aging American Population

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.

TABLE OF CONTENTS

I. Introduction to The Privacy Implications for New Technologies

This article focuses on one subset of the Internet of Things (IoT)[1] revolution, home monitoring technologies, particularly as they affect the elderly, including disabled elderly, populations using these devices and systems in their homes. The selection of these technologies for focus at this point in their timeline of development and usage 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 in IoT, the "canary in the coalmine."[2] While we may see these devices as necessary and desirable for vulnerable populations, once they become available beyond the early adopters, 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, e.g., "home automation systems that turn on your front porch

[1] The Internet of Things refers to the "interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data." OXFORD DICTIONARIES, http://www.oxforddictionaries.com/us/definition/american_english/Internet-of-things (last visited Apr. 27, 2015).

[2] Joseph Lorenzo Hall, the chief technologist at the Center for Democracy and Technology (CDT) explains: " . . . there can be amazing benefits, but at the same time, there is a potential for some serious harm, especially in telehealth and health applications. I consider that sort of the canary in the coalmine for the Internet of Things. If bad things start happening with telehealth 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." FED. TRADE COMM'N, INTERNET OF THINGS WORKSHOP, at 177, ll. 12-20 (2013), http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf ("IoT Workshop" hereafter).

> 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 threefold, in that there is (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 government action as a reflection of society as a whole. Will regulation protect U.S. consumers, or are there other solutions (at least in the meanwhile)?

First, in evaluating these technologies, we should 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

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

[4] Referring to Samsung's acquisition of SmartThings, a home appliance management platform, "'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.'" Max Chafkin, *41. Samsung, For Bringing Internet Intelligence to More Things*, FAST COMPANY (Feb. 9, 2015), http://www.fastcompany.com/3039597/most-innovative-companies-2015/samsung. SmartThings is a "Silicon Valley startup [that] offers a kit that makes it easy for consumers control Schlage door locks, GE lightbulbs, Sonos sound systems, and, as a result of the acquisition, all of Samsung's smart appliances." *Id. See also* Figure 1, *infra,* at 53.

prohibitive,[5] versus purchasing a small device, even with monthly fees.[6] Thus, the home monitoring system may be both more flexible and more cost-effective. Further, empirical studies have shown that older individuals are willing to use home monitoring devices in order to age in place, and "[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]

Next, we should question the amount of privacy that actually is offered up to these new technologies. There is some room for individual variance, but 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 fall alert device in order to get the job done. 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.[8]

[5] Based on 44 hours per week by 52 weeks, the annual estimate 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] *See, e.g., infra*, at 7 (section herein with hypothetical of consumer purchasing device and associated monthly fees).

[7] 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).

[8] "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 for the height of autonomy which is to remain in the home." 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). 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

At the onset of use of home monitoring technologies, there may be differential concerns for privacy regarding the types of data (e.g. temperature of the home versus insulin levels), and much of existing law revolves around which data is sensitive and which is, arguably, 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.[9] There will be less of a distinction in sensitivity of information when all of it is combined in a single platform. Ultimately, the increasing ability of data processors to capture multiple data points and either enter them into algorithms and/or combine these isolated data elements into a complete picture of a person, or and identity, may soon moot this distinction. 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 long beyond the immediate time and place, and even the present-day user. A simple transactional analysis of entering your

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.

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

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, and it 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 imagine 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 fed into the machines results in a collective, conscious intelligence that surpasses what humans can do or control. But before we leap into the future, it will be useful to examine the existing privacy options and implications of home monitoring devices from the perspective of a hypothetical user of such devices.

To illustrate the ideal of balancing individual privacy with physical safety, we can examine a hypothetical example of an elderly patient in need of home monitoring, at the onset of her decision to gather information about her home and herself. In this scenario, "Grandma Bianca" represents a composite yet typical consumer of home monitoring services, in need of some support but not yet ready to completely give over her autonomy to an automated system. We'll consider carefully how to maximize her privacy at each decisional juncture.

Grandma Bianca woke up this morning with slight chest pain. She wasn't extraordinarily concerned as it wasn't like the last time she felt significant chest pain. The last time, almost five years ago, she felt a crushing pain across her chest and a sense of overwhelming dread. That time, she struggled across the room, picked up the receiver of her landline phone, and dialed 911. The ambulance came and took her to the hospital, where she was treated for a minor heart attack and released soon thereafter.

After that incident, she had several experiences of minor chest pain, and each time she thought about calling 911, but hesitated due to the cost of an ambulance visit and the resulting tests in the ER. What if it was just heartburn? But what if it wasn't?

Several of Bianca's friends relied on their cell phones for emergencies. Bianca, however, was concerned that she might not be able to dial the phone, even a single number, in a true emergency, and that she might not be able to effectively communicate that there was an emergency. And how would they know who and where she was?[10] She needed to purchase a device to identify and locate her, at least when she was alone in her home.

Last year, Bianca decided to buy a two-way communications device called a Personal Emergency Response System (PERS). She opted for a company that offered the

[10] "There are 4 basic problems calling 911 from a cell phone:
1- They don't know WHO you are: The caller ID from your cell phone does not identify who you are, only your phone number and possibly a general metropolitan area where your cell service originates from. They will not know your name, home address, medical condition or who to call in the event of an emergency.
2- They don't know WHERE you are: 911 responders don't immediately know where you are – the closest they know is the location of the cell service tower you used when placing your call. If you lose connection or drop your phone before you have given your location, they may not be able to find you.
3- All cell phones DO NOT send GPS coordinates. Your phone may have a GPS feature on it, but that information may not be sent to 911.
4- When an accident, emergency or medical situation occurs, finding the buttons and dialing an emergency number could be difficult under stressful situations. Having a 1-button operation solves this problem."
SKYANGELGPS, http://www.skyangelgps.com/ (last visited Feb. 6, 2015).

local rather than the national system, so her call would go to the large city near her house rather than a call center in Milwaukee or Omaha. They sent her a receiver that plugged into the phone outlet, and a rather unobtrusive button-activated pendant that would send a signal to the receiver, which would call the local call center instead of 911.

So far, she had only pushed the button once, but it had worked pretty well. It wasn't even for chest pain. She slipped in the bathroom and landed hard on her tailbone, pushed the button, and spoke aloud to the receiver. They answered relatively quickly and the service coached her through a way to roll to the side and, reaching for the edge of secure countertop, slowly rise to a standing position. They did not call 911. The kind voice on the other end of the line also asked Bianca several questions tailored for Bianca's particular health condition, including asking if she had taken her heart medication.

If Bianca had said nothing, the call center had her address, and even the ability and authority to "seize the line," or interrupt a busy signal.[11] For an additional fee, Bianca could add "check-in calls, wake-up calls, medication reminders, and language translation"[12] to her basic PERS service. So far, she felt that she didn't need those extra services, but she might in the future. Bianca had considered the language translation service, as her first language was Spanish, but she decided her English was good enough as she had lived in the U.S. for most of her adult life.

[11] Kate Rauch, *A Buyer's Guide to Personal Emergency Response Systems*, CARING.COM, https://www.caring.com/buying_guides/personal-emergency-response-system-guide.
[12] *Id*.

Bianca looked into buying just the device without the monthly service, but she worried about bothering her son and his wife, who had a new baby, with a late-night call. The device would only call her programmed emergency contacts[13] without reaching a 24-hour call center or service.

Bianca was also tempted to add the option for automatic voice messages in case she couldn't speak.[14] This concerned her, however. What if she hesitated and it spoke for her before she could say what she wanted? What if the standard message didn't apply to her situation? This seemed like too much automation for her current health status, and she wasn't ready to let someone else speak for her.

She wondered how the call center personnel decided whether to call 911, especially if she didn't specifically request that they do so.[15] What kind of information did the service have beyond what she had provided them?[16] Did the kind voice

[13] "Priority for SOS call - block all incoming calls during SOS mode- SOS call will continue until it is answered by a human- Answering machines will not fool this system. Able to detect answering machine / voice mail from a human . . . When the panic button is pressed, the system dials the first number that is programmed into it. The system then waits to 'hear' the '#' button pressed on the other end of the line. This tells the system that a human answered the call. If the system hears a '#' it will stop calling numbers and will turn on the speakerphone. If the system does not hear that a '#' was pressed, it will then hang up, and call the next number in sequence. We suggest that you optionally have 911 programmed at the end of the call list to ensure that someone is contacted in the event of an emergency." *Medical Alert Systems*, ASSISTIVE TECHNOLOGY SERVICES, http://www.tntalert.com/ (last visited Feb. 6, 2015) ("ATS Alert Systems" hereafter).

[14] "Q. What if I have a stroke and cannot speak? A. This system has the answer. When the system is activated, it plays an outgoing message to the person receiving the call, letting them know there is an emergency. It speaks for you!" *Id.*

[15] "AlwaysThere4U™ assures you that someone will be there to take a call. Once you connect with the Care Center and *it is decided that emergency services are needed* [italics added for emphasis] the Care Center will contact 911 or other services on your behalf based on your need." *Medical Alert Monitoring*, ASSISTIVE TECHNOLOGY SERVICES, http://www.assistivetechnologyservices.com/medicalalertmonitoring.html (last visited Feb. 6, 2015).

[16] "What type of information does a LifeStation Care Specialist have access to?
Only the information that you have provided. They have access to such information as your address, best route to your home, medical response agencies, your contact list and any hidden key / lock box information." *Medical Alert Questions*, LIFESTATION, http://www1.lifestation.com/faq.php#q33top10 (last visited Feb. 6, 2015) ("LifeStation Top 10 Qs" hereafter).

answering her call have any medical training, or any emergency response training? She hoped that they did, but she wasn't sure.

How will the emergency personnel access her home? Doors can be automatically accessed, with different levels of security. On the most basic level, the consumer can outfit the door lock with a lockbox, and the call center can provide the combination to emergency personnel.[17]

This time, Bianca decided not to push the button, but felt better knowing that she could. Bianca slept well that night, or at least slept better than she had before she bought the system. She decided that the system was money well spent, but still wondered what information the PERS system kept about her and her family and visitors. She hoped that the next generation of devices protected her privacy as well as her health and safety.

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. Section I of this paper introduced the concept of privacy for the relatively new technologies of home monitoring, Section II will review the existing law as it applies to these technologies, Section 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

[17] "If you are concerned about your contact people not being there in time, we recommend ordering a LifeStation Lock Box. The LifeStation Care Specialist will provide the lock box key door combination to the responding medical personnel allowing them to gain access to your home without doing damage." *Id.*

technologies like telephony, and Section V offers concluding remarks and suggestions for future research.

II. Existing and Privacy Solutions for Home Monitoring Devices, Services, and Applications

A. Privacy and Technology, Past and Present

Privacy law in the United States has arisen in response to new technologies that invade the home and its private sphere without stepping through the doorway. At privacy law's inception, "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 first responded to the invention of the instant camera and its use by the press to report on society figures. The second responded to the development of wiretapping technology."[18]

Nevertheless, the privacy right at issue for home monitoring is not the right to be left alone.[19] It is difficult to function in a modern, data-driven economy without offering some of your own data into the collective. The right of privacy we are trying to

[18] Benjamin Wittes, *Database: Digital Privacy and the Mosaic,* THE BROOKINGS INSTITUTION (Apr. 1, 2011), http://www.brookings.edu/research/papers/2011/04/01-databuse-wittes#_ftnref8.
[19] *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890); and the continuing stand on the issue in *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

define, identify, and protect is closer to the right to control access to personal information, and to rights of notice and consent/choice for the distribution of such information.[20] It's the right not to have your own data extracted from your private life come to attack and abuse you, a concept one scholar has termed "databuse."[21] Thus, we need to move away from legal precedents that consider the home the boundary for personal privacy and towards legal frameworks that reflect the technologies we have, which allow for access to the home and to private information in unprecedented ways.

1. Monitoring Privacy from Home Base

To access the home and its wealth of private and perhaps valuable data, home monitoring companies are moving into a sacred space, as a person's home is her "castle,"[22] and she the queen of this domain and its primary decision-maker. Diving into history, "the house of everyone is to him as his castle and fortress, as well for his defence against injury and violence, as for his repose."[23] It has come time to consider whether the castle's threshold, both literally and figuratively, can hold back the onslaught of privacy intrusions.

Into the early 21st century, privacy in the home has been given significant judicial deference in evaluating whether a Fourth Amendment search and seizure

[20] 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.

[21] "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." Wittes, *supra* note 18.

[22] First legal mention of home equals castle is found in *Semayne's Case*, 77 Eng. Rep. 194 (K.B. 1603).

[23] *Id*.

violation has occurred. In *Kyllo v. United States*,[24] 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, and home monitoring may at some point become ubiquitous. If so, would listening to someone's home monitoring devices be like looking in an open window? Yes, if it's a greenhouse not the residence per se,[25] but No, if it's 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."[26]

The state's corresponding obligation to respect the home's "well-being, tranquility, and privacy" is an interest "of the highest order in a free and civilized society."[27] Now uncontroversial, "Supreme Court justices of all stripes today accept that the Fourth Amendment reaches beyond the technology of the 18th Century and requires application to today's analogous intrusions."[28]

[24] *Kyllo v. United States*, 533 U.S. 27, 40 (2001).
[25] *Florida v. Riley*, 488 U.S. 445, 450-51 (1989).
[26] *Florida v. Jardines,* 133 S.Ct. 1409, 1414 (2013).
[27] 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 (1980) (citing *Carey v. Brown*, 447 U.S. 455, 471 (2010).
[28] Wittes, *supra* note 18. *See e.g., Kyllo, supra* note 24.

Corporate policies reflect this legal precedent. Nest devices monitor home temperature, among several other data points,[29] and the company headlines a section of its privacy policy with "We believe home is a private place."[30] The home monitoring technologies used by Nest are new enough that we can believe the intention, but whether the data stays inside the home after it is collected is another matter entirely. From a home safety perspective, Nest is assuming that more data is better,[31] although it may not be that more data is better if third party marketing agencies and/or government entities can access and subpoena that information. It will be interesting to see what the courts make of requests for data by government entities from third-party data collectors of home monitoring data.[32]

[29] "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" *Privacy Statement for Nest Products and Services,* NEST (Jun. 17, 2015) https://nest.com/legal/privacy-statement/ (last visited Jul. 28, 2015) ("Nest Privacy Statement" hereafter). Oh, and "*[t]hey can also sense whether something in the room is moving*." *Id.* (emphasis added). "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." *Id.*

[30] Of course, there's more. The Privacy Policy itself says, "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." *Privacy Policy for Nest Web Sites,* NEST (Jun. 17, 2015), https://nest.com/legal/privacy-policy-for-nest-web-sites (last visited Jul. 28, 2015).

[31] "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." *[FAQs] About Nest Aware with Video History*, NEST (Jun. 18, 2015), https://nest.com/support/article/Frequently-asked-questions-about-Nest-Aware-with-Video-History (last visited Jul. 27, 2015). The Nest Aware service now saves video for future review with video history subscription with up to 30 days saved for review.

[32] Nest's parent company, Google, has received six stars, a perfect score, in fighting data requests. Nate Cardozo, et al., *Who Has Your Back?* EFF (May 15, 2014), https://www.eff.org/who-has-your-back-2014 (last visited Apr. 30, 2015).

2. Routine Stealth Government Surveillance

Government entities can subpoena data, or they can access using less transparent and more direct methodologies. From the government, we've begun to see a shift in the use of monitoring technologies from what the police can do on the own, to a "piggybacking" on more advanced corporate technologies.[33] Police departments can, and will, use third-party contractors to access a wider variety of surveillance techniques, including cameras, which can monitor public streets, and possibly workplaces and homes.[34] At some point in the near future, or perhaps already, we need to our judicial system to include in its interpretation of the Fourth Amendment and its constitutional companions the relationship between the government and its corporate subcontractors to ascertain what is left of individual privacy.

The first legal defense for privacy in the U.S. has been based on individual authority to contract, including notice of uses and implied or ideally explicit consent to those uses of personal data. Issues of notice and consent, and the transparent and understandable transmission of that information, are central to privacy rights in the

[33] "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." Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1311 (2012).

[34] "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." David Sasaki, *SeeChange* (Mar. 3, 2014), http://davidsasaki.name/2014/03/seechange/.

U.S.[35] This right of control may falter when presented with a heavier weight on the other side of the scale. We need to consider what happens when the issue of privacy versus technology becomes not one merely of access, but an issue of life and death, and that value must be weighed against the privacy rights of the individual. Even in life and death situations, there remains a need to consider the value of privacy, and create devices and systems that allow each individual or family to make a decision about privacy and autonomy.[36]

B. Regulation of Home Monitoring Devices

Who's minding the store on home monitoring devices and their interconnectivity with local and worldwide networks? If we are comparing IoT monitoring to human monitoring, the scale is weighted heavily towards human in-home health care if the primary concern is whether the industry is sufficiently regulated. Regulations for human in-home care spans health and financial concerns.[37] Historically, government agencies have monitored portions of the technology, but no one agency

[35] According the current White House policy, "consumers have a right to easily understandable information about privacy and security practices." 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, White House Press Release (Feb. 23, 2012), available at https://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.

[36] "Both in the home and in the investigator's 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." 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).

[37] *Home Care Regulatory Issues,* NAT'L ASSOC. FOR HOME CARE & HOSPICE, http://www.nahc.org/advocacy-policy/home-care-regulatory-issues/ (last visited Jul. 28, 2015).

was tasked with looking at the ecosystem, including for security or privacy as a whole.[38] Thus, statutory support for consumer privacy in monitoring devices exists only in part or by analogy. In order to achieve a fully-regulated industry, "[t]he FTC's standard . . . may mean that in the end all biometric and sensor-based Internet of Things data need to be treated as PII. That, however, would require a radical re-working of current law and practice."[39]

Unlike the heavily regulated 911[40] and telecommunications industry, the home monitoring and PERS industries are largely unregulated.[41] Training for personnel receiving alert or alarm calls may be standardized, or quite minimal, but in any case, is market-driven rather than regulated.[42] There are both state and federal regulations that address broader issues that cross-sect home monitoring devices, including laws governing health care, financial data, and data breach. Federal legislation has been

[38] Jay Radcliffe, a senior security analyst for InGuardians noted that, "no 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." IoT Workshop, *supra* note 2, at 184, ll. 11-20.

[39] Scott Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 132 (2014) (relying upon FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012)).

[40] 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 Mar. 8, 2015). The company's products only extend from enterprise to small and medium businesses, but not consumer use.

[41] "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." 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.

[42] "What kind of training do LifeStation Care Specialists receive? All LifeStation personnel begin their 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." LifeStation Top 10 Qs, *supra* note 16.

proposed to address privacy on a grand scale, but it is not only lacking in teeth but perhaps also a mouth[43] in that the regulations proposed are merely suggestions, not black letter law.

So much of our privacy landscape has been built upon the foundations of U.S. squeamishness about revealing financial and 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."[44] 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.[45] Therefore, if the entity gathering health data is not a covered provider such as a hospital or medical care

[43] 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 . . . ." White House Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015, at 1 (proposed Feb. 27, 2015), available at http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf ("White House Draft: Consumer Privacy Bill of Rights Act" hereafter). 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.

[44] HIPAA Privacy Rule, U.S. DEP'T OF HEALTH & HUMAN SERVS., available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html (last visited Apr. 29, 2015).

[45] Joseph Lorenzo Hall of CDT explains: "And one of the big problems here is a lot of consumer-facing health applications aren't governed by HIPAA. 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." IoT Workshop, *supra* note 2, at 179, ll. 16-23 (2013).

provider, there's no protection from HIPAA. If the data is not medical data, there's no protection from HIPAA.

U.S. privacy law strongly values the individual and personal nature of financial information. However, the FTC dismisses the Fair Credit Reporting Act as a potential check on the unlimited collection and use of data from IoT devices in noting that, " . . . the FCRA excludes most 'first parties' that collect consumer information; thus, it would not generally cover IoT device manufacturers that do their own in-house analytics. Nor would the FCRA cover companies that collect data directly from consumers' connected devices and use the data to make in-house credit, insurance, or other eligibility decisions – something that could become increasingly common as the IoT develops."[46]

The FTC also notes that its own jurisdiction is limited,[47] and calls instead for federal legislation on privacy and security for the Internet of Things. Nevertheless, the FTC promises that it " . . . 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."[48]

[46] IoT Connected World, *supra* note 3, at 17.

[47] "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." *Id.* at 50-51.

[48] *Id.* at 53.

Without a coherent federal data breach strategy, the states have stepped in to provide various data breach laws, with varying standards. But no state or federal law addresses home monitoring data or IoT data overall, protects it, or requires IoT data breach notification.[49]

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."[50] However, this privacy restriction is relegated 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 analogy when discussing standards for notice and transparency for elderly and disabled users in the solutions section of this article.

[49] "Thus, for the vast majority of states, a security breach that resulted in the theft of records containing users' names and associated biometric or sensor data would *not* trigger state data-breach notification requirements. A breach that only stole sensor data without users' names would also fail to trigger such laws." Peppet, *supra* note 39, at 137 (emphasis in original).

[50] Americans with Disabilities Act, 42 U.S.C. § 12112(d)(3)(B), available at http://www.gpo.gov/fdsys/pkg/USCODE-2011-title42/pdf/USCODE-2011-title42-chap126-subchapI-sec12112.pdf.

In addition, the Children's Online Privacy Protection Act (COPPA)[51], the California erasure law, and other age-based statutes may also serve as useful analogies for developing privacy protections for the aging population. 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, or that there are consequences to 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 or plans 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 particularly 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

[51] 15 U.S.C. §§ 6501-06, available at http://www.coppa.org/coppa.htm (last visited Jul. 27, 2015).

is still seen as invasive.[52]. Also, IoT data may be subpoenaed in cases related to end-of-life and estate decisions made by family members as well as insurance companies. In order to create an ecosystem of privacy and security for these devices, we'll have to look first to the companies themselves.

C. Industry Standards

If there is no comprehensive regulation, or none to speak of, our next hope for protecting consumer privacy would be industry standards. In fact, there's been some movement towards industry standards and the establishment of best practices in lieu of government regulation. When companies institute privacy by design and security by design, according to the FTC staff report on IoT, "[a]s part of the security by design process, companies should consider: (1) conducting a privacy or security risk assessment; (2) minimizing the data they collect and retain; and (3) testing their security measures before launching their products."[53]

Privacy industry standards include de-identification of personal data,[54] encryption, and data minimization. Data minimization alone contains several recommendations and concerns within this single industry standard. For instance, data

[52] "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 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." Peppet, *supra* note 39, at 136-37.

[53] IoT Connected World, *supra* note 3, at iii.

[54] De-identification is an imperfect science, to say the least, according to Paul Ohm in *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010). Further, "[e]very successful reidentification, even one that reveals seemingly nonsensitive data like movie ratings, abets future reidentification." *Id.* at 1705.

can be collected later, or companies can destroy data no longer in use. The FTC staff report explains that, "staff's recommendation on data minimization is a flexible one that gives companies many options. They can decide not to collect data at all; collect only the fields of data necessary to the product or service being offered; collect data that is less sensitive; or de-identify the data they collect."[55] Data minimization in theory works, but often fails in practice, e.g. listening TV picks up everything said in the room not just "turn on TV"[56] and transmits it to the Internet. The essence of home monitoring IoT is that it is constant monitoring, and corresponding, 24/7 data collection. Data minimization is not unique to IoT devices in general or home monitoring specifically, but it is much more crucial given the vastness of collection.

When large collections of data aggregate on identifiable platforms or within targetable databases, the danger of breach escalates. New data breach laws in California and perhaps at the federal level promise notification post-breach, but plans for preventing access and breaches remain elusive. Further, recommendations for data protection regulations in the U.S. have focused on the collection and storage of large databases,[57] whereas the information collected by home monitoring devices, while highly sensitive, may be collected by smaller providers and slip again through the gaps

[55] IoT Connected World, *supra* note 3, at iv.

[56] "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." 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/.

[57] *See* Ohm, *supra* note 54, at 1760. *See also* The Personal Data Notification & Protection Act, at 2 (proposed Jan. 12, 2015), available at http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf (last visited Mar. 9, 2015) (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").

in data breach and related regulation. 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.

III. Mass Market Consumer-Focused Home Monitoring

A. Security Ecosystems for Home Monitoring Devices

When we're trying to find out how private data is within a system, we'll need to look at how secure the system itself can be. Data security and privacy are triggers to evaluate the effectiveness of the service to see if it is a sturdy backbone for privacy protection. One PERS company has issued a bare-boned proclamation that it has, at least, redundancy of systems in the event of a single call center failure.[58] This is a moderate acknowledgement that things can go wrong, but not the full-fledged security program necessary for effective data security.

The FTC met in November 2013 to hear comments on the Internet of Things, and issued a staff report in January 2015. In that interval, home monitoring established a toehold in at least the early adopter American household. The commenters focused on three areas of harm as follows: "participants noted that the IoT presents a variety of

[58] Assistive Technology Services has specific representations with regard to physical data security as follows: "We have invested heavily to accomplish 100% redundancy between our two alarm central stations to make sure that our customers won't go unprotected due to power failures, storms, or other disasters. This redundancy includes the protection of facilities, data, receivers, and telephones. Many alarm central stations in our industry claim to be fully redundant, but in reality, most are only data redundant. To complement our redundancy, our facilities are also equipped with standby generators that contain multiple independent fuel sources, allowing us to provide continuous alarm monitoring services despite equipment failures, storms, or outages." ATS Alert Systems, *supra* note 13.

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."[59]

There are exponential security issues in a distributed system vis a 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/storage of data.[60] The 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.[61]

[59] IoT Connected World, *supra* note 3, at ii.

[60] Lee Tien of the Electronic Frontier Foundation (EFF) summarizes this point as follows: "[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 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." IoT Workshop, *supra* note 2, at 71-72, ll. 11-25, 1-6.

[61] Jeff Hagins, the cofounder and chief technology officer at SmartThings, the startup that connects things in the physical world to the Internet, explains the multiple standards, but it all comes down to the security of the home wifi network, as follows: "One is a standard called Zigby and the other is a standard, pseudo-standard called Z-wave. These are both mesh networking standards that are wireless, different frequencies. Zigby is 2.4 gigahertz and Z-wave is a 900 megahertz ISM standard, but these are RF standards. At the end of the day, Zigby and Z-wave actually end up being potentially more secure than wi-fi [but] device providers tend to rely on the home network itself as the security boundary, as the only security boundary. Once you get that device connected to your wi-fi network, that's it. And if you have security on your home network, then that's the security. And if you don't have security on your home network, then there is none whatsoever, right? But once the device is connected to that network, that is the only security." IoT Workshop, *supra* note 2, at 101-02, ll. 20-25, 1-15. Hagins further explains that, "if you have a wireless router, pretty much anything made since 2007 has this little push button on it. And the whole idea behind it was that, hey, end-users can't set-up stuff securely, even if they use the right, you know, encryption, like the strongest encryption, they choose a weak pass-phrase because it is something that they are trying to remember. So the idea was look, you push a button on your router, you push a button on whatever you want to connect to your wireless network, and they automatically exchange, in a secure manner, this network key so this device can connect to your network. So you can have a very long, auto-generated, very random password that you don't have to remember. The problem is that that technology, WPS, was itself broken. And so attackers can come along and break WPS and then, oh yeah, here's the network key.

What can go wrong when home network security is breached? First we might look at cameras, the eyes and often ears of home monitoring, both for the security of individuals and property. The FTC chair noted that, in "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."[62]

Traditional malware, viruses, and worms can infest a home network, either incidentally or specifically targeted[63] to home monitoring devices. One worm studied "can be utilized by the attackers to perform distributed denial-of-service (DDoS) attacks."[64] At that point, denial of service could wipe out an entire system, leading to shut down of power, light, or other connected systems in the home.

There's not much in the way of financial incentives to build IoT devices with even the most basic security envelopes, and some older hardware harbors legacy malware such as the "Misfortune Cookie."[65] In most cases, there's a counterincentive to

And so now it doesn't matter how secure -- how good your encryption is, I have the encryption key and I can decrypt everything." *Id.* at 103-04, ll. 6-25, 1-3.

[62] IoT Workshop, *supra* note 2, at 13, ll. 1-6.

[63] "The attacker was in a position to begin attack these [sic] devices at a time of their choosing", 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 (last visited Mar. 9, 2015).

[64] *Id*.

[65] "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." Robert Vamosi, *Attack of the Home Router,* DARKMATTERS (May 27, 2015), http://darkmatters.norsecorp.com/2015/05/27/attack-of-the-home-router/.

make the security open, e.g. allow a back door[66] for customer service fixes and upgrades. Such openings are quite well known in the security community.[67] The consequences may be alarming, and regulators have taken notice of the potential for breaches or simply use of publicly available private data for unintended purposes.[68]

Breach and failure analysis must be included in any evaluation of the efficacy of a home monitoring system. What happens when the system is breached, data is leaked, or the system simply goes offline? A failsafe mechanism, or default protocol, should be baked into the system so doors and windows remain secure.[69]

There's also the trade-off between security and safety. Security and safety, in many people's minds, are synonymous. However, when there's a two-factor authentication methodology to access the system (very secure), there's a delay in uploading data to the system, which may decrease the level of safety, in say, an emergency response system. In the home monitoring scenario described in the

[66] A list of home router models with backdoors was started at https://github.com/elvanderb/TCP-32764/blob/master/README.md (last visited Jul. 20, 2015).

[67] Craig Heffner, a security researcher with Tactical Network Solutions, a cyber intelligence company, with a focus on embedded infrastructure security illustrates: "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." IoT Workshop, *supra* note 2, at 74-75, ll. 18-25, 1-10.

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

[69] Marc Rogers, who is the Principal Security Researcher at Lookout, Inc., a mobile security company, explains that "at 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 open, and therefore people would be able to walk into your house." *Id.* at 348-49, ll. 19-25, 1.

hypothetical earlier in this article[70] and other similar situations, the risk of security leaks is not just that privacy may be compromised, but that life and limb are in danger. Similarly, the FTC notes in its report on the Internet of Things that, "unauthorized persons might exploit security vulnerabilities to create risks to physical safety in some cases."[71]

Looking to hack devices connected from people's homes to the Internet? Searches can be performed online.[72] Searches can be done by anyone, including those with profit and with political motives. Increasingly, security in the home is the foundation for national security.

B. Connections: Security in the Home, Law Enforcement, and Homeland Security

While this paper will address primarily the implications of corporate data collection and disclosure to the public, it is proper to note the potential for government monitoring that may result from the tempting collection and storage of data in the private sphere. At this point, many home monitoring devices are simply uploading data to a server rather than providing real-time data and data analysis to the consumer. Access is therefore limited to the company providing the device and, with some limitations and delay, to the consumer who is providing the data to the company.[73]

[70] *See supra*, at 7.

[71] IoT Connected World, *supra* note 3, at 12.

[72] *See* SHODAN, http://www.shodanhq.com (last visited Mar. 9, 2015).

[73] Eric Lightner, the program manager for Advanced Technology Development at the Department of Energy and Director of the Federal Grid Task Force, explains that " . . . in a smart meter, there is really

However, the future of law enforcement and government surveillance may be access to these previously private sources of data formerly only available to and in the private sphere. Beyond the scope of this paper but of great interest to Fourth Amendment scholars and law enforcement agencies would be the use of near real-time analytics of the mass of this data to go beyond alerting paramedics to individual emergencies such as a pending stroke to alerting the city services about group emergencies such as heat stroke due to a power failure.[74]

As noted by Lee Tien from EFF, 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."[75]

Similarly, the potential for cyberterrorism squeaks in at this low, home-based level in a way few anticipate when they purchase a thermostat or other home

two radios, right? One radio that communicates your usage back to the utility for billing purposes. And a radio that is usually turned off, or that is always turned off, for now, that would communicate the usage directly to devices in your home. And that currently is a function that is not utilized to date. So to really get access to your energy usage information, you usually go through a web portal that the utility has set up and that's password protected and it's your account information and that's how you usually get your usage information. It's usually a day late, so today is Monday, that usage won't really be available until the next day, on Tuesday, for you to see. So it's not in real time, that would be the advantage of having communication directly with the meter, into devices. It would become more a real-time look at your usage, but for now, it is the next day." IoT Workshop, *supra* note 2, at 85, ll. 1-21.

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

[75] IoT Workshop, *supra* note 2, at 68, ll. 10-18.

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."[76] Similarly, access to home monitoring devices can have the same devastating consequences if left available for hacking and other malfeasance.[77]

We're in big trouble 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.[78] In addition to data collected by devices connected to the Internet, consumers are entering much of the private data collected by the home monitoring devices. One example would be in naming the devices, or the sets of data, including using consumers' and their children's names.[79] Have any home monitoring systems

[76] *Id.* at 304, ll. 17-22.

[77] Jeff Hagins of SmartThings notes the interesting discrepancy between devices that seem to need security, and those that seem not to need security, but surely do when one considers the consequences of the lack thereof: "Meaning that connected 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." *Id.* at 105, ll. 5-16.

[78] "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")." Joseph Lorenzo Hall, *The Beginning of the End of Passwords,* CDT (Oct. 21, 2014), https://cdt.org/blog/the-beginning-of-the-end-of-passwords/ (last visited Apr. 28, 2015).

[79] Jeff Hagins of SmartThings finds that "the consumers actually add contextual data into the systems. So with our system as an example, 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

been hacked yet? Yes, they have.[80] However, as of 2014, hackers who were able to access Nest devices did so with physical, in-person access to the devices, rather than remotely. Stay tuned as the possibility of remote and system-wide hacking remains, perhaps imminently. Homeland security (we hope) has stronger passwords, but the federal government may fail to realize its citizens' security is dependent on this fundamental weakness in home security.

Home and personal monitoring for seniors and persons with disabilities presents system-wide as well as individual risk. Instead of just attacking a single person's pacemaker or insulin pump, pervasive hacking of a home monitoring system such as Nest or a PERS system could result in multiple deaths. Similar to a heat or cold wave, temperature changes could cause risks to elderly or disable patients. Likewise, a denial of service could cause relied-upon security and communication systems to go offline for a significant amount of time.

C. 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, often not just alarm or alert

childrens' names and whether they are in their room or not. It's very, very private information." IoT Workshop, *supra* note 2, at 88-89, ll. 17-25, 1-3.

[80] For a grand and comprehensive of list of IoT devices that have been hacked, and how, see: 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.

monitoring companies, but also advertising and marketing companies. Access to the home for data and data use by home monitoring devices threatens privacy. For example, interconnected devices are able not only to collect data, but also to upload and distribute it. Distribution of data may be made to third parties or simply to other locations of companies that are doing the collection. Third-party distribution is likely to result in targeted advertising.[81]

Mass-market home monitoring extends beyond thermostats and refrigerators. In fact, the most pervasive home monitoring may be in the form of entertainment devices such as televisions and gaming consoles.[82] Gaming consoles collect consumer data from the gamers for the purposes of establishing an account, and then myriad data points for the game play. In particular, there are newer, more emotive interfaces for voice and gestural input that provide more "personal" data.[83]

In the near future, it will be safe to assume that a smart home appliance or monitoring device is a computer rather than the reverse, as "some of our engineers view a refrigerator really as a 72 inch computer, right, that just happens to keep your

[81] Ryan Calo of the University of Washington Law School gives a pertinent example: "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." IoT Workshop, *supra* note 2, at 364, ll. 9-15.

[82] Our hypothetical Grandma Bianca could have been quite the gamer in her youth. *See supra,* at 8.

[83] Lee Tien of EFF noted that, "[b]ut 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." IoT Workshop, *supra* note 2, at 86, ll. 12-22.

food cold."[84] Each and every connected device captures vast quantity 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 significant quantities of data, so much that camera companies are giddy with desire to use the data in new and interesting ways.[85]

Smart appliances, on the whole, require us to enter personal data. The popularity of 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 nearly instantaneous return on your investment. The needle will move on your valuable personal comfort – you will feel the warmth of connection, of safety, or just of the air in the room. The smarter a consumer wants the device to be, the more of her identity or her personal information she must feed it.

The quantity of data created by even a small subset of home monitoring devices connected to the Internet is enormous.[86] To compile the data, at this point there are

[84] *Id.* at 59, ll. 4-6.

[85] "'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?"'" 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 (quoting CJ Prober, GoPro's senior vice president of software and services). The article further speculates "[t]hat 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." *Id.*

[86] Jeff Hagins of SmartThings explains: "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

more devices communicating with the network than individuals communicating with the network, and the number of connected devices is increasing rapidly.[87] The number of devices connected to the Internet has been facilitated by the move from IP v4 to IP v6 and the greater capacity for IP addresses[88] to associate with each device. Further, the ability to capture not only large quantities of data but to process such data in real time[89] compounds the need to address privacy concerns at this juncture.

We can assume as well that an individual consumer, on average, does not need to decide whether they would like her room to remain at a comfortable temperature. There is a baseline need, or at least desire, for personal comfort and ease of use. 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

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." IoT Workshop, *supra* note 2, at 89, ll. 3-10, 14-22.

[87] Edith Ramirez, Chairwoman of the FTC reiterated: "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 . . . ." *Id.* at 7, ll. 10-23.

[88] Vint Cerf, Vice President and Chief Internet Evangelist for Google explained: "[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." *Id.* at 142, ll. 20-23.

[89] "[D]ata analysis is increasingly conducted in speeds approaching real time." White House Interim Progress Report, Big Data: Seizing Opportunities, Preserving Values, at 2 (Feb. 2015), available at https://www.whitehouse.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf.

some enthusiasm for Apple brand iWatches."[90] Watches, in particular, are a familiar mode of technology interaction for older generations of individuals, and therefore may 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.[91]

The television is now also a home monitoring device. Cnet noted in February 2015 that "[i]t sounds like something straight out of George Orwell's 1984. Samsung's Smart TV privacy policy, which most people never bother reading, reveals that your shiny new television set may be capable of spying on you. Samsung 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.'"[92] The key issue here is not just that data is being captured in the home, but that it may be automatically captured without individual action, and that it may be transmitted to third parties without a secondary notice related to the latter transaction.

What if the data is being provided not only to the homeowner, the homeowner's trusted circle, and the company/provider, but beyond those expected groups, to, say,

[90] During the final stages of the initial draft of this paper, Apple released the Apple iWatch, widely touted as a "life saving device." 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. Query whether wearable self-monitoring devices will replace home monitoring systems entirely or merely interact with them.

[91] "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." *Lively 24/7 Emergency Medical Alert System*, LIVE!Y, http://www.mylively.com/how-it-works (last visited Jul. 29, 2015).

[92] 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/.

the neighborhood? 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 consumers to 'make better decisions about how they use electricity.'"[93] It doesn't take a vivid imagination to go beyond insulation levels to the greater quality and quantity of data collected by IoT devices and say that other such data might and may be shared with the neighbors. A standard model of notice and consent for use may not be able to encompass the potential uses and misuses of this data.[94]

D. Notice and Consent for Marketing Use

Standard notice and consent requirements are overbroad in the sense that they ask for notice and consent where the consumer may not necessarily be interested. Few consumers read notices and fewer read them thoroughly. However, they are 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.[95] For example, 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

[93] IoT Connected World, *supra* note 3, at 8 (internal citations omitted).

[94] *See* Section E, *infra,* at 41 for further discussion of imaginable misuses.

[95] Marc Rogers of Lookout, Inc. speculates that, "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." IoT Workshop, *supra* note 2, at 322, ll. 14-22.

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."[96] This is arguably beyond a camera's obvious purpose, and may lead to a host of "surprise" uses of the data yet to be imagined.

Concurrently, the information is provided as a continuous flow rather than in bursts of information provided at a doctor's visit or even with a digital transmission by the consumer.[97] When this information is provided continuously, there are fewer opportunities for user interface and input, and therefore fewer opportunities to interact with the consumer and obtain consent for use of their data. 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 is the paramount concern, but 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?[98] And two, how do we provide notice

[96] Nest Privacy Statement, *supra* note 29.

[97] Vint Cerf of Google explains: "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." IoT Workshop, *supra* note 2, at 123, ll. 6-13.

[98] Jeff Hagins of SmartThings notes "[w]hereas 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." *Id.* at 98-99, ll. 21-25, 1-8.

when there's no user interface on the device?[99] User interface notice and consent procedures may have to be re-formulated to encompass notice on multiple platforms (app, device, smartphone, console, laptop).

Third party use is covered in some privacy policies and terms of use, but not all. One of the most intense concerns is around the use of personal data in the home for insurance purposes, either ostensibly by an insurer providing the device and collecting the data, or by the insurer "piggybacking" on existing data, perhaps even making the disclosure of such data a precondition to obtaining insurance or obtaining a lower rate for existing service.[100] In early 2015, an insurer offered customers exactly that deal.[101]

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

[99] Lee Tien of EFF noted that, "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." *Id.* at 99, ll. 12-25.

[100] Scott Peppet, a professor at the University of Colorado Law School: " . . . you 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?" *Id.* at 211, ll. 14-22.

[101] 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/.

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.

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? If someone other than the user has purchased a system for a disable patient, who is the user for authentication and access purposes? Data retention presents a somewhat lesser burden for elderly than for college students, who are fully in possession of many of the rights and responsibilities of adults but have los the right to be forgotten erasure laws for under 18 year olds.

What happens in IoT devices when there's no obvious user interface? 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."[102] Particular attention will need to be made to addressing 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.

[102] IoT Connected World, *supra* note 3, at v.

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."[103] Conversely, the latest bill proposed by the current administration proposes that if the use is exactly what the customer asked for, we should presume notice and consent and be done with it.[104]

E. Imagined Harms for Unimagined Uses

There's also an economic twist in evaluating this home monitoring "upgrade": will it be an elite system, in which only the rich benefit from smart houses and high-quality personal care? Perhaps, or, conversely, the poor may be monitoring more intensely, either through "voluntary" economic incentives or individual necessity.[105] There is very little regulatory prohibition of economic discrimination based on the collection of data through home monitoring devices, as long as it is accurate.[106] 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 by their unfamiliarity with new technologies in the case

[103] *Id.* at vi.

[104] "Personal data processing that fulfills an individual's request shall be presumed to be reasonable in light of context." White House Draft: Consumer Privacy Bill of Rights Act, *supra* note 43, at 8.

[105] Scott Peppet of U. of Colo. L. Sch.: "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 more than everybody else." IoT Workshop, *supra* note 2, at 212, ll. 8-12.

[106] " . . . the 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. " Peppet, *supra* note 39, at 128 (emphasis in original).

of the elderly, or their difficulty in using the technologies in the case of elderly, and the necessity of using the technologies in both cases.

A new bill proposes to at least address this issue of "disparate impact" in analyzing personal data and using it against individuals or groups.[107] 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 that prevent true transparency and privacy rights against advertisers.[108]

Is there an absolute harm for unimagined uses? Perhaps consumers would like to be delighted and surprised by new uses that will improve 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 option. A company could offer proposed future uses in the notice, but would these be construed as contracts? So far, privacy notices have not been held to a contract standard.[109] Further, devices from multiple sensors in

[107] "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 " White House Draft: Consumer Privacy Bill of Rights Act, *supra* note 43, at 9.

[108] *Our Data, Our Rules?,* THE BRIAN LEHRER SHOW (Jan. 6, 2015), http://www.wnyc.org/story/our-data-our-rules/ (last visited Apr. 28, 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).

[109] *See Dyer v. Northwest Airlines Corp.*, 334 F. Supp.2d 1196, 1200 (D.N.D. 2004). *See also* Daniel Solove and 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).

the home can be combined to create new and highly intricate portraits of individuals.[110] In that sense, nearly every use is a surprise, an unintended use, if it can be combined with other data and/or transferred to third parties via bankruptcy, merger, or acquisition.

There has been extensive focus on the potential negative consequences of third parties accessing data, particularly for purposes beyond which the person generating or providing the data intended. However, it is also interesting to speculate, or in many cases simply observe, what the effect of collecting and analyzing the data may be on the individual generating the data. In some cases, the effect will be immediate, such as when an aberrant temperature in the home creates an alert that causes the home's resident to change/normalize the temperature, either through manual adjustment or through a preset, programmed response. Normalization is the effect of collection and data analysis on an individual basis and, increasingly, may be the effect of autonomous use of the collected and analyzed data as more data is available on home monitoring devices. A "normal" value may be set by the user, or, eventually, by the system as a default.

Privacy is still important to older users of home monitoring devices, but the calculation may result in a different decision, as follows. Privacy is always an individual calculation, perhaps cluster-able by type across multiple spectrums, but in the case of elderly users, the ability to be identified and located is an important value if the purpose

[110] "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.'" Peppet, *supra* note 39, at 93 (internal citation omitted).

to get immediate attention. Individually worn healthcare devices can identify individuals with great certainty.[111] As of this writing, wearable devices are luxurious rather than necessary for functioning in society. 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 chose 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.

The FTC, and indeed the entire U.S. government, stance on the issue of privacy and security relies on the assumption that educating the consumer will solve every flaw in the system. In fact, consumers may not fully be aware of security flaws or be able to fix them even if their awareness of such issues is fully developed.[112] The solution may be to make consumers aware of the issue, but rely on developers to close the security gaps.[113]

IV. Privacy Solutions

[111] Scott Peppet of U. of Colo. L. Sch.: "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." IoT Workshop, *supra* note 2, at 170-71, ll. 24-25, 1-2.

[112] Craig Heffner of Tactical Network Solutions explained: "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." *Id.* at 77, ll. 4-17.

[113] Heffner further explained: "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." *Id.* at 77, ll. 18-21.

A. Waiting for Developer Knights in Shining Armor

What can developers do before products hit the market to prevent privacy violations and security breaches? The magic 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 user error and hacking outside of acceptable parameters for the device.[114] Technical standards for secure design are available online and updated frequently.[115] As a foundational matter, companies should hire security personnel (not just generic software developers) to design these programs. And before that, universities must educate developers to design products that are not only beautiful and clever, but also secure.[116]

In theory, consumers would only buy secure products that are protective of their privacy. In practicality, market information on this subject is scant and unreliable. Worse yet, there always will be certain consumers who choose less secure devices because they are cheaper to buy or to operate, or cuter, or endorsed by a celebrity, or any other reasons one could assign to human frailty. Therefore, designers of secure IoT

[114] Mike Beyerle of GE Appliances: "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." *Id.* at 106, ll. 10-17.

[115] *See Standards for M2M and the Internet of Things, Published Specifications,* ONEM2M (Jan. 1, 2015) http://www.onem2m.org/technical/published-documents (last visited Mar. 9, 2015).

[116] *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).

solutions to be used in 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 device engineering's concerns,[117] it should at least be on the developers' 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 their offerings, but also developing instructional videos explaining how to use these options and posting them on YouTube.[118] Both developers and consumers can access and use these 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.

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, and companies can offer privacy-protective products and services, but ultimately the future of privacy and security will be consumers paying attention to and paying for privacy, preferably

[117] "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." 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.

[118] *See* Microsoft, *Quick Tutorials*, YOUTUBE (Feb. 6, 2015), https://www.youtube.com/playlist?list=PLtSVUgxIo6KoI5ogCBZuAjB6HprjiaKNM (last visited Apr. 29, 2015).

privacy protections that have been incorporated into consumer products via privacy 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, we are looking for a home-based solution, assuming that there will not be aggressive and imminent legislation on this issue, and assuming no 100% secure solution will be offered by developers.

Generally, home monitoring devices are on the lax end of the spectrum, and specifically, one study found that ten out of ten devices allowed rudimentary passwords. In addition, if they have password thresholds at all, then there is a need to notify or even require customers to re-set default passwords. Individually, 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.[119] Consumers can limit the amount of data entered into the device, a sort of data minimization on the ground level. Consumers can also use biometric or other alternatives to passwords, such as encryption for uploaded video feeds[120] and other protection of data in transit to ramp up privacy protections, or at least confuse hackers until this methodology, too, is compromised. Indeed, consumers of IoT equipment can

[119] "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 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." Nest Privacy Statement, *supra* note 29.

[120] Describing a new video home monitoring service: "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." 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/.

interconnect their devices to a secure platform, or at least a secure home network.[121] Even 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, either by individual consumers themselves, by consumers through add-on products, or by companies providing home monitoring devices in a holistic solution.[122] One company offers a layer device on top of the home network for precisely that purpose.[123] Platforms that manage home security and monitoring systems are proliferating, offering users additional choices to make initially, but hopefully simpler choices down the road with regard to privacy notices. Ideally, privacy notices will offer the user a choice to revoke or revise their privacy level elections as their understanding or situation changes. In the situations raised by this article, our hypothetical Grandma Bianca may well want to revise her privacy elections as her health changes, as she adds

[121] Simple instructions are available online for making a home network more secure. *See How to Secure Your Wireless Home Network*, WIKIHOW, http://www.wikihow.com/Secure-Your-Wireless-Home-Network (last visited Apr. 29, 2015).

[122] Joseph Lorenzo Hall of CDT explained: "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." IoT Workshop, *supra* note 2, at 216-17, ll. 12-25, 1.

[123] Bitdefender Box promises the following comprehensive solution: "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." BITDEFENDER, http://www.bitdefender.com/box/ (last visited Feb. 13, 2015).

additional authorized users to the system, or as she adds additional devices that necessitate platform-level management.[124]

Still, there are limitations on a platform-level security barrier, including the ability of apps to collect data outside platform parameters and the need to pre-identify known threats.[125] Data anonymization as a principle has some utility but 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" time and money 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. The Business Associate agreement, for example, provides for flow-down of obligations to unregulated companies that are in the data stream. In the transcript of the FTC workshop on IoT, Lee Tien of EFF noted that, for a California proposal, "[w]e

[124] *See supra,* at 7.

[125] "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." 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.

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."[126]

HIPAA regulation, established in 1996, was expanded in 2013 to encompass business associates who contract with covered entities as well as the entities themselves.[127] HIPAA could be expanded again to include under its regulatory umbrella any business that captures, processes, and stores health data. Under this scenario, at least 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 data emanating from home monitoring devices collecting personal health information.

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, and protect the security of data so that health care monitoring and support devices would function properly.[128]

[126] IoT Workshop, *supra* note 2, at 70, ll. 4-7.

[127] "The HIPAA Privacy and Security Rules have focused on health care providers, health plans and other entities that process health insurance claims. The changes announced today expand many of the requirements to business associates of these entities that receive protected health information, such as contractors and subcontractors." Press Release, HHS Press Office, New Rule Protects Patient Privacy, Secures Health Information (Jan. 17, 2013), available at http://www.hhs.gov/news/press/2013pres/01/20130117b.html.

[128] "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." IoT Connected World, *supra* note 3, at vii-viii.

At the time of this writing, several bills are pending at the federal level to create a coherent scheme for protecting data and establishing breach notifications. Home monitoring privacy legislation may be too specific, and even IoT privacy legislation may be too specific to gain broad-based political support.[129] One proposal, from the White House, suggests that covered entities for privacy protections be expanded to include any "person that collects, creates, processes, retains, uses, or discloses personal data in or affecting interstate commerce,"[130] 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.[131]

V. Conclusions and Next Steps

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. Still, we will have to decide as a society where home monitoring devices fit on the scale of importance, from equivalent to national security to the lesser standard of disposable and recreational gadgets.

Now, not after a significant breach of security and violation of individual privacy rights, is the time to evaluate potential regulation and alternatives to regulation of home

[129] " . . . 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." *Id*. at vii.

[130] White House Draft: Consumer Privacy Bill of Rights Act, *supra* note 43, at 1.

[131] "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)." *Id.*

monitoring, including the ability of users of all ages to participate in these alternatives. At this point, consumers have begun to weigh the options presented to them in the world of IoT, and its entry into their homes. Truste noted that 22% of consumers believe that the benefits of IoT devices outweigh the risks to privacy.[132]

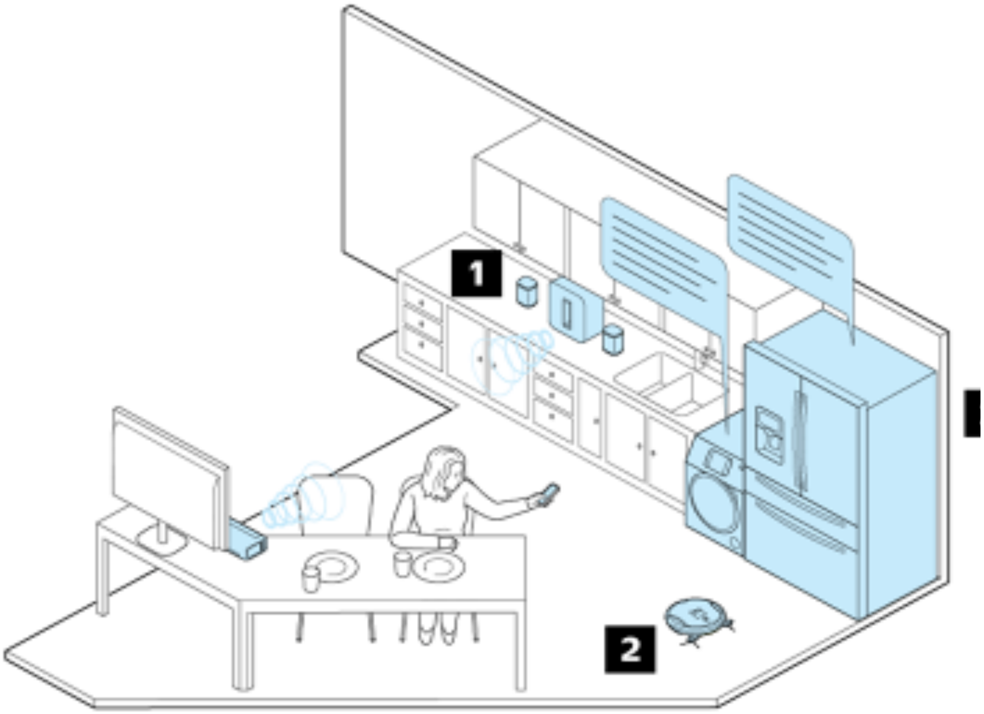
To begin, some people might opt out of using home monitoring devices, preferring to incur the cost of human care and monitoring that is more expensive by several orders of magnitude, choose less invasive devices that gather information but do not transmit the information to the Internet,[133] or buy into the panoply of IoT devices but use commercially-available or home-grown privacy protection devices.

[132] *TRUSTe Privacy Index: 2014 Internet of Things Edition*, TRUSTe (2014), available at http://www.truste.com/resources/privacy-research/us-internet-of-things-index-2014/ (last visited Mar. 6, 2015).

[133] The author of this paper has a non-IoT pedometer. Occasionally, they wear it.

Illustration of Smart Home Technologies

Figure 1:[134]



1 Open platform: SmartThings connects Samsung devices, but also to Schlage locks, GE lightbulbs, Sonos, etc.

2 Universal control: Users can manage Samsung's robot vacuum with a smart-watch, Galaxy, or (gasp) iPhone.

3 Contextual smarts: A refrigerator that texts when the door's open; a washer cycles when it's cheapest to do so.

[134] Chafkin, *supra* note 4 (illustration by Colin Hayes).