The Ethics, Privacy, and Legal Issues around the Internet of Things
W231: Spring 2015
Kelsey Clubb, Lisa Kirch, and Nital Patwa

1. Introduction

At its base, the "Internet of Things" (IoT) is a system of sensors, CPUs, and wireless radios connected to the Internet. Economies of scale are enabling IoT devices to be produced at a low cost for consumer use in homes, cars, and wearables; the ubiquity of wireless networks is enabling the continuous data from these devices to be sent, processed, and stored in the cloud. These IoT datasets are carrying a rich variety never seen before. When they are combined with external datasets, a surprising list of possibilities emerge. To name a few:

- From a smart-phone connected wearable device: detection of sensitive behavioral patterns, mood, habits, stress levels, personality type, progression of Parkinson's disease, bipolar disorder.
- From a connected-home: times when the home is vacant, times when only elderly or children are at home, does the occupant cook dinner.
- From a connected-car: what are the driving habits, which places does the driver routinely visit.

Thus, IoT is not just the internet of "things." It is the internet of "mind, body, and soul." It is the internet of "behavior." It is the internet of "life."

Tim O'Reilly, founder of O'Reilly media who coined the terms open source and Web 2.0, recently pointed out that the Internet of Things goes beyond the "hype of new gadgets that light up Kickstarter campaigns, and pack the halls of consumer electronics conferences." As the combination of powerful, low-cost sensors become ubiquitous, mass adoption of mobile gadgets that serve as hubs for IoT devices, blazing fast wireless networks, and all the data these things generate come together, O'Reilly says "This wave of technology has more chance of reimagining whole swathes of the world than anything we've seen before. This is really going to disrupt everything.[1]"

[1] O'Brien, C. (2015, March 4). Tim O'Reilly: Silicon Valley is massively underestimating the impact of IoT (interview). Retrieved April 20, 2015, from http://venturebeat.com/2015/03/04/tim-oreilly-silicon-valley-is-massively-underestimating-the-impact-of-iot-interview/

While these new datasets bring benefits of disruptive proportions, their richness and variety also brings the means to harm as never seen before. For example, sensitive behavioral patterns could be used against a person for life-insurance, employment, lending, or renting decisions without transparency or detection. Driving habits could be used against a person for auto-insurance decisions. Home vacancy and occupancy information could be used by intruders.

The “terms of use” or “consent” that consumers sign before using IoT devices and services are typically not comprehensible by most consumers. In practice, most of the consumers sign the these terms giving companies broad rights of collection, sharing, and use that consumers probably never would have given, had they understood the potential harms they could cause.

Therefore it is of utmost importance that we review IoT; understand the limitations of protective legal and regulatory frameworks, and provide actionable recommendations to maximize the good and minimize the harm.

1.1 Major IoT Markets

We will begin by introducing three major IoT areas: Connected cars, connected wearables, and smart homes.

1.1.1 Connected Cars

A car has an intricate electro-mechanical system for its core driving functions consisting of engine, braking, acceleration, battery, transmission, lights, wipers, GPS, and more. It has a safety system consisting of airbags, antilocking brakes, collision warning system, blind spot detection, radar, and camera-based object detection system, to name a few. Then it has a driver personalization system consisting of position controls of seats, mirrors, head-rests, entertainment system, and climate control system.

In the near future every new car will have (1) Internet connectivity to connect these systems to cloud-based applications (2) a state-of-the-art ad hoc wireless connectivity to (a) other vehicles in the vicinity (b) sensors on the road, on signal lights, and on street traffic signs; all collectively called ad hoc-wireless-connected-components (3) a black box to record continuously the data generated by internal systems. The black box will be able to record the data coming from internet-connected cloud applications, or from ad hoc-wireless-connected components. By the same token, data recorded on the black

box will be accessible by internet-connected cloud applications and to ad hoc-wireless-connected components.

The vision of connected cars is transformative. Connected cars can enhance safety, improve adherence to traffic rules, reduce congestion on the roads, and enhance the driving experience. However, the dataset generated by connected cars with its rich history (from days to years) and the rich variety (from location to acceleration to braking) carries huge amounts of private information with vast predictive powers. Therein lies the concern. The dataset is used by both the applications in the car and the applications in the cloud. Who owns this dataset and who has access to this dataset? What are the business practices of the companies that have access to the dataset? In what manner is the dataset is being used and being shared? In addition, there is a grave safety concern if unauthorized users hack into the connected car systems.

1.1.2 Connected Wearables

Another major IoT market is connected wearables. These can take many forms, the most common of which is something you wear on your wrist (such as a Fitbit activity tracker or an Apple smartwatch), but other emerging wearables are in the form of eyewear (similar to the recently discontinued Google Glass) or even clothing, such as a t-shirt. This is a rapidly growing market with the IDC (International Data Corporation) reporting that, "vendors will ship a total of 45.7 million units in 2015, up a strong 133.4% from the 19.6 million units shipped in 2014. By 2019, total shipment volumes are forecast to reach 126.1 million units, resulting in a five-year compound annual growth rate (CAGR) of 45.1%."[2]

A significant amount of information can be collected by these wearables, information that would otherwise be time-consuming and possibly less accurate to record and collect. A Jawbone or Fitbit fitness tracker is intended to be worn on the wrist nearly 24/7 (except while charging or swimming) and both collect information on your activity (e.g., how many steps you took each day and at what time of day), your sleep (e.g., what time you fell asleep, what time you work up, how many times you woke up), and more advanced models can collect your GPS location information (e.g., the route you took while running or cycling) and even your 24/7 heart rate. There are also apps

[2] Press Release (2015, March 30). Worldwide Wearables Market Forecast. Retrieved April 27, 2015, from http://www.idc.com/getdoc.jsp?containerId=prUS25519615

associated with each device that allow you to track what you eat and drink and, if you pair the app with a wireless scale, you can keep track of your body weight, too.

The collection of all of this data is primarily for the use of an individual user. The combination of information about sleep, nutrition, and exercise (quality and quantity) is geared toward helping the user be the best he or she can be by helping them reach goals whether the goal is to lose or maintain weight or to train for a triathlon. Companies like Jawbone have created a team of data scientists that also use the aggregated data from all Jawbone users to help find trends in the data (such as how does location East or West within a time zone affect what time people go to sleep[3] and what factors help people lose weight[4]) and even tries to coach you on what to change[5]. This is an example of the sum of the individual parts benefiting the users as a whole. Apple's Research Kit[6] is also just starting to use the data collected by these wearables to help research in healthcare and Jawbone has now introduced the ability to use its UP4 as a mobile payment device[7]. Future use cases for this kind of data could include things like connecting heart rate data to home sensors[8] and maybe even connecting your health data with your online dating profile (to "prove" you really are as active as you claim to be).

There is some concern that wearable data could get sold to insurance providers who could then justify raising health insurance costs to users who do not eat healthily or exercise much, or that employers could gain access to the data to see that their

---

[3] Nolan, T. (2014, October 7). Dance to the Circadian Rhythm. Retrieved April 27, 2015, from https://jawbone.com/blog/circadian-rhythm/

[4] Nomura, E. and L. Borel. (2015, April 8). Weight Loss: What Really Works. Retrieved April 27, 2015, from https://jawbone.com/blog/weight-loss/

[5] Nomura, E. and B. Wilt (2014, November 4). Smart Coach: Getting to Know Your Workout: Retrieved April 27, 2015, from https://jawbone.com/blog/workout-tracking/

[6] Loria, K. (2015, March 10). Apple is Ushering in a 'New Era' of Medical Research. Retrieved April 27, 2015, from http://www.businessinsider.com/apple-researchkit-could-transform-medical-research-2015-3

[7] Olivarez-Giles, N. (2015, April 16). Jawbone Puts Mobile Payments Into New UP4 Fitness Band. Retrieved April 27, 2015, from http://blogs.wsj.com/personal-technology/2015/04/16/jawbone-puts-mobile-payments-into-new-up4-fitness-band/

[8] Tso, R. L. (2014, October). Smart Homes of the Future Will Know Us by our Heartbeats. Retrieved April 27, 2015, from http://www.wired.com/2014/10/smart-homes-of-the-future/

employee was out on a run while he or she had called in sick. There are all kinds of possible issues surrounding ownership of data, transparency of use, privacy, and security[9], and it is imperative for companies that produce wearables to have plans in place ahead of time that address these issues and the unforeseen issues that come with these devices being connected to many other apps and devices.

1.1.3 Smart Homes

As home automation evolves to monitor and control mechanical, electrical, and electronic systems - such as controlling lighting, heating, air conditioning, ventilation, appliances, windows, locks, communication systems, entertainment systems, and home security devices - it improves convenience, comfort, energy efficiency, and security[10]. For instance, in the programmable world of interconnected devices, when your garage door closes as you leave, it could also turn off the lights and adjust the thermostat to save energy, a dog tag could text you when your dog leaves the yard, the moisture sensors in the lawn can tell the sprinklers to turn on after checking the forecast to predict water requirements, when your car gets close to your home, it could adjust your lights, stereo, temperature, and window shades to your preferences before you walk in the door, your swimming pool heats up when there is a barbecue on the calendar[11]. Our adaptive environments become connected spaces that will be able to retrieve and use contextual, relevant, timely, and accurate information to interact with us[12].

Navigating the competing standards for home automation (X10, Zigbee, Z-Wave, WiFi, Bluetooth, Insteon, KNX, UPB) and vendors (Ingersoll-Rand Co.'s Nexia Home Intelligence System, Schneider Electric SA's Wiser Home Management System, AT&T's Digital Life automation system) can be overwhelming and costly since most of these rapidly changing technologies do not seamlessly integrate easily. Consumers have a

[9] Blum, B. and K. Clarke. (2015, January 18). Are Your Wearables Safe From Cyber-Security Threats? Retrieved April 28, 2015, from http://www.accenture.com/us-en/blogs/technology-blog/archive/2015/01/18/are-your-wearables-safe-from-cyber-security-threats.aspx

[10] Internet of Things. (n.d.). Retrieved April 20, 2015, from http://en.wikipedia.org/wiki/Internet_of_Things

[11] Wasik, B. (2013, May 14). In the Programmable World, All Our Objects Will Act as One | WIRED. Retrieved April 20, 2015, from http://www.wired.com/2013/05/internet-of-things-2/

[12] Baker, A. (2015, February 5). Connected spaces: The next step for the internet of things. Retrieved April 20, 2015, from http://www.theguardian.com/media-network/2015/feb/05/connected-spaces-should-be-the-next-step-for-the-internet-of-things

range of stand alone products (SmartThings, Lowe's Iris, Belkin's WeMo, Wink), ecosystems of products, and home automation systems by professional installers (Crestron, Vivint, Control4, Elan, Frontpoint, Savant, ADT Pulse) to choose from. Devices that monitor environmental conditions such as energy, water, and temperature can eventually pay for themselves. Enthusiasts can even swing by the Home Depot or Lowes and pick up or order online from smarthome[13], littleBits' electronics smart home kit[14] to link up their own devices or create their own linked scenarios by using IFTTT[15] (If-This-Then-That), or even just monitor how much power their house and gadgets use with Neurio[16].

In the rush to get products to market, often the security of these home automation products has been overlooked. David Bryan and Daniel Crowley, security researchers at Trustwave Holdings, have shown that a lot of these devices, such as Veralight, do not require any authentication at all or even when authentication was turned on, it could easily be bypassed[17]. Bruce Schneier, Chief Technology Officer at Co3 Systems, points out (1) that since chips are cheap and profit margins are slim for embedded systems, companies do as little engineering as possible before shipping, (2) software is old, even when the device is new, and (3) no one entity has any incentive, expertise, or even ability to patch the software once it's shipped - maintaining older chips and products just isn't a priority[18]. Billy Rios, founder of Laconicly LLC and security researcher, demonstrated at the RSA Conference how an attacker could abuse a cross-site request forgery (CSRF, a flaw originally reported in 2013 by TrustWave SpiderLabs) in the Vera

[13] Smarthome Home Automation Superstore. (n.d.). Retrieved April 20, 2015, from http://www.smarthome.com/

[14] Smart Home Kit. (n.d.). Retrieved April 20, 2015, from http://littlebits.cc/kits/smart-home-kit

[15] IFTTT. (n.d.). Retrieved April 20, 2015, from https://ifttt.com/

[16] Finley, K. (2015, February 26). This Tiny Gadget Tells You Exactly How Much Power Your House and Gadgets Use | WIRED. Retrieved April 20, 2015, from http://www.wired.com/2015/02/tiny-gadget-plugs-house-monitors-power-use/

[17] Metz, R. (2013, August 13). More Connected Homes, More Problems. Retrieved April 20, 2015, from http://www.technologyreview.com/news/517931/more-connected-homes-more-problems/

[18] Schneier, B. (2014, January 6). The Internet of Things Is Wildly Insecure — And Often Unpatchable | WIRED. Retrieved April 20, 2015, from http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/

Smart Home Controller to completely own the device, as well as infiltrate the home network and attached computers[19].

As David Gerwitz, one of America's foremost cyber security experts, asks "How many of us, when we were growing up, had to install updates on our lightbulbs? Or reboot the TV? Or add security updates to a refrigerator?[20]" Kamin Whitehouse, an associate professor at the University of Virginia who studies smart buildings, says "even if data traffic from wireless smart devices in the home is encrypted, an attacker can still analyze network traffic patterns and, by making a few assumptions about human behavior, get an idea of what's going on inside the house.[21]" The main security disaster is when "hackers figure out that it's easier to hack routers than computers.[22]"

Even when used as intended, devices can also perform in unexpected ways. Raul Rojas' "smart home" froze up, and stopped responding to his commands - it turned out that one light fixture had burned out, and was trying to tell the hub it needed attention. It did this by sending continuous requests that overloaded the network and caused it to freeze in a "classic denial of service attack" in the effort to say "change me.[23]"

Redundancy and checks need to be designed into IoT devices and systems. For instance, what if a sensor goes bad and is sending out incorrect information and suddenly your refrigerator orders a bunch of unnecessary items? Or what if during a hack of a chain pharmacy's network, your forgetful grandmother's medication

---

[19] Higgins, K. (2015, April 16). Popular Home Automation System Backdoored Via Unpatched Flaw. Retrieved April 22, 2015, from http://www.darkreading.com/vulnerabilities---threats/popular-home-automation-system-backdoored-via-unpatched-flaw/d/d-id/1320004

[20] Gewirtz, D. (2015, March 18). Internet of things: Sillier and scarier and coming your way | ZDNet. Retrieved April 20, 2015, from http://www.zdnet.com/article/that-internet-of-things-siller-and-scarier-and-coming-your-way/

[21] Metz, R. (2013, August 13). More Connected Homes, More Problems. Retrieved April 20, 2015, from http://www.technologyreview.com/news/517931/more-connected-homes-more-problems/

[22] Schneier, B. (2014, January 6). The Internet of Things Is Wildly Insecure — And Often Unpatchable | WIRED. Retrieved April 20, 2015, from http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/

[23] Hill, K. (2015, March 3). This guy's light bulb performed a DoS attack on his entire smart house. Retrieved April 20, 2015, from http://fusion.net/story/55026/this-guys-light-bulb-ddosed-his-entire-smart-house/

management system[24] inadvertently advises her to take the wrong dosage sending her wearable glucose and blood pressure monitor into a tizzy sounding alarms so much that she turns it off severing the link with her insulin pump and possibly subjecting her to diabetic shock. What if an elderly person is at home alone and one sensor alerts that she has fallen, should the sensor "call" an ambulance or should there be multiple sensors needed before sending an alarm?

1.2 The IoT Leads to New Ethical and Legal Questions

This leads to questions of:

- What happens when the Internet connection goes down?
- What if the IoT product vendor's services experience downtime at a critical juncture or for critical life supporting devices?
- Is there a guarantee for security/hacker-proofing on the cloud side of IoT services to prevent nefarious access to a home's internal network[25]?
- Who is responsible or liable for patching IoT devices, routers, and cloud connections?
- What happens if the IoT product vendor goes out of business and no longer supports the product?
- Who owns the data generated and collected by these connected devices?
- With much of the communication occurring between devices without the user knowing, or possibly understanding, what happens when a device chooses to act independently of its owner or acts in unintended ways - from ordering the wrong products, to vacuuming at an unreasonable hour, to misinterpreting facial expressions or gestures and responding appropriately?
- Are there situations where these devices should not be collecting data?
- What about those who do not have smart devices or the knowledge to use them? "Digital knowledge divide"
- What if the consumer wants to opt out?

Are any of these questions addressed by current laws and/or guidelines? We'll look into that next.

---

[24] Coughlin, J., & Yoquinto, L. (2015, March 15). The Very Old Will Be the Guinea Pigs of the Internet of Things. Retrieved April 28, 2015, from http://www.slate.com/articles/technology/future_tense/2015/03/elderly_users_will_be_the_guinea_pigs_of_the_internet_of_things.html

[25] TS, G. (2015, April 17). Home Automation Systems - A Consumer Checklist. Retrieved April 20, 2015, from http://www.anandtech.com/show/9174/home-automation-systems-a-consumer-checklist

2. Current Laws and Guidelines Applicable to IoT

2.1 Laws

We currently have a range of laws protecting the data of US citizens. IoT data usage is always subject to fairness and anti-discrimination laws for the protection of civil rights for lending, employment, and housing governed by the Fair Credit Reporting Act (1970)[26], the Equal Employment Opportunity Act (1972)[27], and the Fair Housing Act (1968)[28]. If the IoT data is consumer-generated, it is not subject to HIPPA (1996)[29], but if it is generated in conjunction with a healthcare provider, it is protected by HIPPA. If the subject for which data is being collected is a minor, then the data is subject to the Children's Online Privacy Protection Act (1998)[30]. The service providers involved in transmitting the data are subject to the Electronic Communication Privacy Act (1986)[31] which does not allow them to see the data; however, they can still see the meta-data. All government agencies and government contractors are subject to the Privacy Act, which is based on the Fair Information Practice Principles (FIPPs) guidelines[32]. Any data security breach is subject to Breach Notification Rule[33], which requires the

[26] Fair Credit Reporting Act. (2012, September 1). Retrieved April 21, 2015, from http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0111-fair-credit-reporting-act.pdf

[27] Equal Employment Opportunity Act. (1972, March 24). Retrieved April 21, 2015, from http://www.eeoc.gov/eeoc/history/35th/thelaw/eeo_1972.html

[28] Civil Rights Division Home Page. (n.d.). Retrieved April 21, 2015, from http://www.justice.gov/crt/about/hce/title8.php

[29] Health Information Privacy. (n.d.). Retrieved April 21, 2015, from http://www.hhs.gov/ocr/privacy/index.html

[30] COPPA - Children's Online Privacy Protection. (n.d.). Retrieved April 21, 2015, from http://www.coppa.org/coppa.htm

[31] Electronic Communications Privacy Act of 1986 (ECPA). (n.d.). Retrieved April 21, 2015, from https://it.ojp.gov/default.aspx?area=privacy&page=1285

[32] Fair Information Practice Principles. (n.d.). Retrieved April 21, 2015, from http://itlaw.wikia.com/wiki/Fair_Information_Practice_Principles

[33] Breach Notification Rule. (n.d.). Retrieved April 21, 2015, from http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/

company to send a notice of breach to all affected consumers. While these laws were not written with IoT in mind, they can be expanded and adapted to cover IoT data.

2.2 FIPPs Guidelines

The data collection and usage is guided by Fair Information Practice Principles (FIPPs). The Code of Fair Information Practices is based on five principles:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

Currently the Fair Information Principles are only recommendations for maintaining privacy-friendly, consumer-oriented data collection practices, and are not enforceable by law. The enforcement of and adherence to these principles is principally performed through self-regulation.

However, Federal Trade Commission (FTC) monitors the companies for their privacy practices to be consistent with what they advertise in their privacy policy, and examines both the policy and the practice for unfair and deceptive practices. The FTC is authorized under the FTC Act (1914)[34] to file a complaint against a company.

2.3 Federal Trade Commission Guidelines

[34] 15 U.S. Code § 41 - Federal Trade Commission established; membership; vacancies; seal. (n.d.). Retrieved April 21, 2015, from https://www.law.cornell.edu/uscode/text/15/41

Recent FTC guidelines[35] cover IoT devices sold to consumers only, not to businesses. IoT devices provide new beneficial services to consumers, improving productivity, health, and safety. In addition, they can provide new information to product developers, healthcare researchers, and the government to yield benefits to society.

The FTC clearly recognized the security risk of unauthorized interception of communication and unauthorized access to the device, the later imposing significant personal safety risks. The FTC recommended that security should be built into the device from the very beginning and tested rigorously. The company should monitor the product through its lifecycle and provide patches for vulnerabilities. Also the consumer should be notified when there is security breach.

If the company is collecting data, the risk to the consumer is that the data will be used in a way different from the consumer's expectations. Consequently, the FTC recommends data minimization: minimizing what data to collect and for how long it is retained.

However, since there are likely to be future beneficial uses of the data, companies may choose to collect more data and store it for longer periods. In such situations, the FTC recommends the approach of "notice and choice" to consumers in a clear and prominent manner, such as within set-up wizards, in a privacy dashboard, or at point-of-sale (not through lengthy documents). If the company is de-identifiying the data at the time of collection, the FTC allows collection of de-identified data without any "notice and choice".

All uses of data must comply with FIPPs and existing laws such as the Fair Credit Reporting Act. The FTC does not recommend a "use-based" approach as a substitute for a "notice and choice" approach because of (1) insufficient legal framework and codes of conduct for this approach, (2) ambiguity around the determination whether the use is beneficial or not, and (3) an increased security and privacy risk associated with increased data collection.

[35] Internet of Things: Privacy & Security in a Connected World. (2015, January 27). Retrieved April 28, 2015, from https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

The FTC advised against IoT-specific legislation, but called for baseline privacy legislation in the US. In the UK and Canada, such legislation already exists[36].

3. Current State of Affairs in the IoT World

3.1 Collection and Control

Examining the data collected by just one connected device, in this case the programmable learning thermostat Nest, we see that Nest[37] gathers information such as zip code (for retrieving weather information), what type of HVAC system you have, whether it is located in a home or business, model and serial number, software version, and battery charge level. nest collects current temperature, humidity, ambient light in the room, when you change the temperature setting and to what, and current state of your HVAC system. In order to work from a smartphone or web interface (browser type and version), as well as download software updates, Nest needs to be connected via Wi-Fi, so stored on the local device are the Wi-Fi network name (SSID), password, and IP address. If you wish to receive energy usage reports from Nest, they have your email address as well. Nest saves your personal information for as long as you remain a Nest customer, backup copies may linger though. The Nest user can access, amend, or delete personal information from Nest's cloud servers through the controls in their account. Nest will share your information with your consent if you sign up for partner energy savings (Rush Hour Rewards), use a service technician, or connect with third-party devices. Nest does comply with the US-EU Safe Harbor Framework and the US-Swiss Safe Harbor Framework with regards to the collection, use and retention of personal information and will respond in good faith if there are legal reasons to provide information. Via their website, Nest also provides information regarding terms of service, end user license agreement, sales terms, etc. As we can see, that is quite a lot of information from just one interconnected device. This could lead to consent fatigue just reading through all of the details.

There is also the question of the accuracy of the collected data and the user's ability to modify it, if needed. Fitbit trackers automatically determine when a user has fallen

[36] Bradbury, D. (2015, April 7). How can privacy survive in the era of the internet of things? Retrieved April 22, 2015, from http://www.theguardian.com/technology/2015/apr/07/how-can-privacy-survive-the-internet-of-things

[37] Legal Items. (2015, February 23). Retrieved April 21, 2015, from https://nest.com/legal/privacy-statement/

asleep and wakes up; Jawbone trackers require the users to push a button to signal when they went to bed and woke up. Fitbit allows users to modify the sleep start and wake times if the user thinks the Fitbit recorded it inaccurately; Jawbone only allows a user to do this if the user forgets to push the button that they went to sleep. So, if I know I looked at my watch at 12:10 am and had not fallen asleep yet, but my Jawbone tracker tells me in the morning I was already asleep by then, then the data it records is inaccurate. Jawbone's data scientists use user's sleep data to make inferences or discover trends. One can hope that on the whole the data is accurate, but inferences drawn from inaccurate data are themselves inaccurate, so there are limitations, especially when you do not allow users to modify their own data.

We would not want people to modify their car's speed data, but what if in the future people are given speeding tickets based on analysis of their car's speed sensors? Those sensors may not always be accurate or there are times where exceeding the speed limit is necessary to avoid a collision. Unless a car has cameras mounted on all angles and the justice system allows those cameras to be used as evidence, the context will not be recorded along with the car's speed and it may be more difficult to contest that kind of speeding ticket compared to when an officer pulls you over and you at least have some chance of explaining the situation.

Another contentious issue with IoT data has to do with data ownership. Does a fitness tracker's manufacture own the data the tracker collects or does the person who creates the data own it? Neither would have data without the other. The consumer does pay the manufacturer for the tracker, but does that cost also include the cost of storing the data and making it accessible in a nice visual format and corresponding app? What about a car's location data? A consumer might not want the car manufacturing company to know the entire list of places he or she has been to since purchasing the car, but would he or she want the location of the car known if he or she got into an accident?

3.2 Usage

The first principle of data usage should ideally be data transparency. Every consumer has a right to know what data is being collected and how it is being used by the company. Few companies do this well, some companies provide some transparency, but a lot of companies are not very transparent at all. Some of this is due to competition and secrecy: Fitbit users might want to know exactly how Fitbit is able to automatically determine when they fell asleep and woke up, but Fitbit might not want to tell users this

as it might give away their methodology in such a way that a competitor like Jawbone could copy it.

Another reason for a company not being 100% transparent is that detailing every single type of data the company collects and how it uses that data could take dozens of pages and several hours for a consumer to read through. There is a trade-off between transparency and consumer burden. This trade-off is also apparent in informed consent and giving consumers choices. Instead of making consumers agree to everything in a terms of use (TOS) or agreeing to nothing, it might be best to allow a consumer to agree to only what he or she thinks is an acceptable use of his or her data. This makes sense for a single TOS, but for dozens, if not hundreds, of TOSs this is a real burden on the consumer.

Assuming consumer's data is allowed to be used by a company, when IoT data is used in aggregate to conduct research, give guidance, or make data-driven decisions, it is critical to be aware of who is included in the dataset and who is excluded in the dataset. Overall, the typical person who is using a connected device--whether it be a Tesla, a Nest, or a Fitbit--is more likely to be richer than poorer. That distinction usually also means there is a division of users based on education, age, race, and geographic location (or some combination). Giving guidance to other users of a device based on inferences from all collected device data is more likely to succeed, but research needs to be reported with the caveat that it only generalizes to the population of users; data-driven decisions that affect non-users must be significantly scrutinized so as to not disadvantage those who have been excluded from the dataset.

There is also the question of whether a user/consumer should have the ability to opt-in or opt-out of his or her data being used in aggregate. Perhaps it is not dire that a person's individual sleep habits are used in global sleep research, but what about the data that would tell an approaching car that your car just hit some black ice and their car should take action to avoid the danger? Where do we draw the line and how do we draw it?

3.3 Access Control, Security, and Standards

Although we are in the early stages of coherent IoT systems, some companies are already envisioning a bigger picture while addressing the needs of privacy and a secure, cooperative future.

Dowse[38] is currently working on solving the problem of opaque gateways via responsible networking and context awareness. The Dowse box is a "device entitlement layer" in the form a box that plugs into the home network and lets the user define what connects with their hub and how. For example, if your new smart meter decides to connect to your utility and tell it things about you, the box would let you know, and give you the chance to do something about it[39]. Bastille[40] prevents airborne threats and flows by checking Radio Frequency (RF) data leakage. The AllSeen Alliance[41] is a nonprofit consortium dedicated to enabling and driving the widespread adoption of products, systems and services that support the Internet of Everything with an open, universal development framework, that does consider security. Ubiquitous Commons[42] is an international research project whose goal is to design a legal and technological toolkit that will allow people and organizations to be able to decide how the data they generate is used[43]. Industry leaders, developers, and product designers are discussing Open APIs, standards, and ethical issues in the first conference on APIs for the Internet of Things, API Days[44] (June 17 and 18, 2015 in San Francisco), the second Solid[45] conference on hardware, software and the Internet of Things (June 23-25, 2015 in San Francisco), and DataEdge[46] (May 7-8, 2015 at UC Berkeley). IEEE[47] has formed a

[38] Dowse - Hub for Local Area Network Awareness. (n.d.). Retrieved April 20, 2015, from http://dowse.equipment/

[39] Bradbury, D. (2015, April 7). How can privacy survive in the era of the internet of things? Retrieved April 22, 2015, from http://www.theguardian.com/technology/2015/apr/07/how-can-privacy-survive-the-internet-of-things

[40] Bastille. (n.d.). Retrieved April 22, 2015, from http://www.bastille.io/about

[41] AllSeen Alliance. (n.d.). Retrieved April 23, 2015, from https://allseenalliance.org/about

[42] Ubiquitous Commons. (n.d.). Retrieved April 23, 2015, from http://www.ubiquitouscommons.org/

[43] Guerrini, F. (2015, April 16). Ubiquitous Commons: How To Regain Ownership Of Your Data In The Internet Of Things Era. Retrieved April 22, 2015, from http://www.forbes.com/sites/federicoguerrini/2015/04/16/ubiquitous-commons-how-to-regain-ownership-of-your-data-in-the-internet-of-things-era/

[44] APIdays SF 2015, the first conference on APIs for the Internet of Things. (n.d.). Retrieved April 23, 2015, from http://sf.apidays.io/

[45] Solid 2015. (n.d.). Retrieved April 23, 2015, from http://solidcon.com/internet-of-things-2015

[46] DataEDGE 2015. (n.d.). Retrieved April 23, 2015, from http://dataedge.ischool.berkeley.edu/

[47] Standard for an Architectural Framework for the Internet of Things (IoT) P2413 Working Group. (n.d.). Retrieved April 23, 2015, from http://grouper.ieee.org/groups/2413/

working group to create a standard for an architecture of IoT. On April 9, 2015, IoTLive [48] had their second virtual conference to solve the unanswered questions of IoT. The Open Interconnect Consortium[49] is defining connectivity requirements to ensure interoperability and open source implementations for wireless connecting devices. The Maker Movement, where inventors, tinkerers, and entrepreneurs test and realize new devices through creativity, rapid prototyping, working around limitations, and using community development to reduce complexity[50], is fueling apps, robots, and IoT[51]. People are moving ahead with these nascent standards, technology, and legal, ethical, and privacy concepts in mind in order to achieve the potential benefits of an IoT world.

3.4 The Internet of Things Bill of Rights

With the knowledge of the limitations of the current laws and guidelines, how can we improve upon what already exists and make further recommendations to guide the future of the IoT?
In 2011 Pachube (currently known as Xively) published an attempt at a Bill of Rights for the Internet of Things[52] as a starting point for discussion:

1. People own the data they (or their "things") create.
2. People own the data someone else creates about them.
3. People have the right to access data gathered from public space.
4. People have the right to access their data in full resolution in real-time.
5. People have the right to access their data in a standard format.
6. People have the right to delete or backup their data.
7. People have the right to use and share their data however they want.

---

[48] IoTLive | #002. (n.d.). Retrieved April 24, 2015, from http://iotlive.org/two/

[49] What Is OIC? (n.d.). Retrieved April 28, 2015, from http://openinterconnect.org/

[50] Mack, J. (2014, June 30). 5 reasons the Maker Movement will drive the Internet of Things. Retrieved April 28, 2015, from http://m2mworldnews.com/2014/06/30/10043-5-reasons-the-maker-movement-will-drive-the-internet-of-things/

[51] OracleVoice. (2014, May 29). Maker Movement Fuels Apps, Robots, And Internet Of Things. Retrieved April 28, 2015, from http://www.forbes.com/sites/oracle/2014/05/29/maker-movement-fuels-apps-robots-and-internet-of-things/

[52] Open Internet of Things Assembly- Postscapes. (n.d.). Retrieved April 20, 2015, from http://postscapes.com/open-internet-of-things-assembly

8. People have the right to keep their data private.

These points include the topics of data ownership, access, deletion, usage, sharing, and privacy, but what about security, transparency, informed consent, and data accuracy? They focus on the rights of consumers, but what about the responsibilities of providers or the possible pitfalls of companies using data to drive decision-making?

4. Our Recommendations

4.1 Design For User Experience, Resiliency, Adaptability, and Security at the Beginning

In order to create well-designed IoT devices developers and manufacturers need to plan ahead for the most likely scenarios, follow standards, use open source architecture and open APIs when possible, and incorporate security and rigorous testing throughout every stage of development, production, and post-production. Rather than focusing on proprietary features, which may run the risk of a VHS vs. Beta battle, or a one-off novelty product in the rush to get to market, designers need to think about how a device can interact and grow along with other potential components in the system.

We also need to think about issues such as how a device can recover gracefully from a power outage, how can it use minimal power, how can it be gracefully phased out in an eco-friendly manner as newer devices become available, and how do you patch an implanted IoT device. Companies have the potential be more profitable in the long-run if they spend time up front thoughtfully designing their products and user experiences.

4.2 Develop IoT Standards

It will be far easier and will permit greater adoption of IoT devices if less time is spent on incompatible, proprietary designs, rather than employing user-friendly plug and play standards. Having a universal standard will allow designers, developers, and product marketers to focus more on user experiences and be able to fulfill the potential for innovation and opportunity. Again, these standards need to cover everything from the technical to the legal and ethical aspects of IoT.

4.3 Simplified Terms of Use & Opt-Out Option for Broader Usage Rights

FTC guidelines recommended “Notice and Choice”, but it seems that “Notice and Choice” as provided by current “Terms of Use” are mostly lengthy fineprints meant to force readers into agreeing to them without understanding them. Due to the sensitive nature, highly predictive power, and the richness of IoT datasets, this practice must not continue. We recommend that the FTC guides the companies to issue simplified “Terms of Use” that clearly spell out any collection, usage and sharing not related to the primary anticipated usage of the IoT device, as well as provide an opt-out option.

4.4 De-identification is Not Enough

Current FTC guidelines allow companies to collect and use data without any consent as long as the collection is de-identified. However, knowing that techniques exist to identify the individuals from de-identified datasets[53] and that non-associated datasets can be linked together in ways that defeat the ability to de-identify, the FTC should require that consent and an opt-out option still be provided and that the risk of identification be spelled out.

4.5 Complete Transparency Even After Consent

Even when consumers have signed the “Terms of Use”, companies should be fully transparent to consumers about what data they collect, who has access to it, how the company uses the data, and how the company keeps the data private and secure. This helps to establish trust between the consumer and the company and a trusting consumer is more likely to allow a company to use his or her individual data for the benefit of all consumers and/or society as a whole. Also, companies must provide consumers a method to revoke the consent at any time and know the implications of a dataset that was collected prior to such revocation.

4.6 Centralized Opt-Out from Data Brokers’ Datasets

[53] Hayden, E. (2013, May 8). Privacy protections: The genome hacker Yaniv Erlich shows how research participants can be identified from 'anonymous' DNA. Retrieved April 24, 2015, from http://www.nature.com/news/privacy-protections-the-genome-hacker-1.12940

With the easy ability to combine various types of data, the “Data Broker” industry of dataset collection, renting, and selling is booming, regardless of whether the data is accurate or not. We recommend that FTC enable a centralized control for all consumers for opting out of all IoT datasets maintained by all Data Brokers. Even though the platform for privacy preferences project (P3P) for permitting users to manage their privacy setting failed, it is possible to learn from its shortcomings and develop a better privacy control system.

4.7 Extend HIPPA to Protect Consumer-Generated Health Data

Since HIPPA currently does not cover consumer-generated health data, there needs to be an extension to protect the consumer.

4.8 Establish Laws to Limit Use of IoT Datasets without Explicit Consent

The FTC is against usage-based consent. However industries such as insurance are eager to use IoT datasets. Since insurance is as essential as credit, employment, and housing, the usage of IoT datasets for insurance decisions must also be regulated and must require explicit “notice and choice”.

4.9 Include Device Override Capabilities

By allowing users to participate in the device decision process it helps to make the application more “contextually aware.” Override capabilities or ways for users to correct the behavior of devices that are acting inappropriately or malfunctioning should be built in to the IoT device.

5. Conclusion

We have provided a comprehensive overview of IoT technology and its implications on consumer well-being. We find that the IoT has many beneficial applications, but current laws and guidelines around the IoT are not strong enough to protect the consumers against adverse or unintended usage. A number of recommendations have been devised and presented to help rectify the situation. Their implementation is intended to

broaden the utilization and usefulness of the IoT, as consumers begin to feel safer and build more trust with this exciting, disruptive technology.