## 

An Analytical Framework and Planned Adaptive Approach for Internet-of-Things Privacy Regulations

17.310 Science, Technology, and Public Policy

04 December 2015

Brandon A. Karpf

ENS USN

## Intro

The Internet of Things (IoT) is an emerging technology that has the potential to improve the world through efficiency and connectivity. It also has the potential to be Pandora’s box. Without a critical evaluation of IoT applications, a well-reasoned analysis of the technology goals, and an engineered regulatory framework, the world will miss out on the full capabilities of this emerging technology, and the results will lead to privacy violations, insecurity, and more.

IoT devices rely on the collection of data, and these devices have the potential to collect highly sensitive and personal information depending on use, context, and processing. Any object or action that takes place within the direct vicinity these consumer devices is a target for data collection. A doorbell camera, for instance, can collect video data of a neighboring house. The collection of data raises significant privacy questions that must be addressed within these contexts. The processing of the data from these sources results in questionable and troubling situations as well. For example, video data can undergo facial recognition, object and product recognition, activity recognition, and deep learning algorithms to predict actions and characteristics of people and places. It is crucial to characterize how the collection, transportation, and processing of this data may conflict with privacy. As it stands, there is currently no definable way to analyze that process. I intend to design and apply an analytic framework to accomplish that goal.

It is not enough to simply analyze this technology; there must also be formal regulation. Industry, government, and consumers must all be made aware of IoT data privacy issues. Companies that develop IoT products currently build operational systems that do not inherently protect privacy. Further, they rely on verbose privacy and use policies. The majority of users will either not read the entire policy or will read it but be unable to properly understand the implications. One consumer study conducted by the Pew Research Center found that only 44% of consumers were aware that the existence of a privacy statement does not necessarily mean that the company intends to protect the confidentiality of any user data.[[1]](#footnote-1) This method of engaging industry and consumers is insufficient. Therefore, I propose a three part regulatory concept based on the analytic framework that should support the various risk management goals in the IoT space. This concept requires the use of the framework to continuously collect market data, the application of the framework for labeling, and a more formal method of government law and regulation as triggered by measurable trends in the collected data.

## Background

IoT represents the largest increase in consumer home technology since the PC and these technologies must be vetted while they are still young. There are currently an estimated 10 billion networked devices ranging from smartphones and tablets to connected cars and wearable technology and that number is expected to more than triple in the next 5 years.[[2]](#footnote-2) The utility of networked devices lies primarily in their cooperation with consumers’ day-to-day lives. Coincidentally, this function is also the most vulnerable to privacy violations. That logic leads to an interesting implication. The function and purpose of an IoT device presents an inherent risk to privacy. This dichotomy arises from the general structure of this technology. IoT devices must constantly collect and process data, often in large quantities. Since most of these devices are not “smart” enough to interpret the data themselves, the data must be shipped back to a centralized server to be processed. It is not hard to imagine the breadth and depth of personal data that can be collected by such a multitude of devices running in perpetuity.

The economic future of IoT seems to be gargantuan, hence the market hype. In one of the more conservative studies, Business Insider estimates that 23.4 billion IoT devices will connect to the Internet by 2019 - 10 billion of which will be driven exclusively by the enterprise and manufacturing sectors. Meanwhile, the most liberal predictions show an estimated 40 billion IoT devices by 2020.[[3]](#footnote-3) Business Insider also claims that an additional $5.6 trillion in value will be added to the global GDP by 2019, with significant savings due to increased productivity in all sectors of the economy: $12 trillion in global manufacturing, $3 trillion in health care, and $800 billion in energy costs.[[4]](#footnote-4) The predicted $200 billion to $350 billion market for in-home IoT products will mostly consist of chore automation, appliance controls, and home security.[[5]](#footnote-5) Meanwhile, 87% of company executives believe that IoT will inevitably lead to consistent job growth that will “change the industrial paradigm of the 21st century.”[[6]](#footnote-6)

There are two models that, when considered together, demonstrate how the IoT technology will lead to market competition, growth, and innovation. However, they also explain the inherent danger that IoT presents to privacy. First, the Power of Technology model is a combination of two theories. The first and most famous is Moore’s law, which has three parts. Computing power doubles roughly every 18 months. Price equivalent capability doubles roughly every 18 months. And research and development costs also double roughly every 18 months. Second, Grove’s law states that successful technology development focuses on technologies that provide an order of magnitude increase in performance, defined as innovation. Therefore, the logical conclusion of this model is that the suppliers drive technology. First, you build cool technology that is fundamentally newer and better than existing concepts. Next, you wait for Moore’s law to bring cost down. Then, a market develops. Finally, market growth is based entirely on sustaining innovations. Large companies with huge research budgets and the ability to swallow losses tend to succeed through this process. A perfect example of a technology in this model is the iPhone. As a company, you must continue to innovate or lose out. This fact will hold true in the IoT realm just as it does throughout information technology.

The second model is where we run into problems. It is called the Disruptive Technology model, and demonstrates an inherent risk to larger firms. A disruptive technology is an innovation that improves a product or service in ways that the market does not expect, typically by being lower priced or designed for a different set of consumers. There are two types. Low-end innovations target customers who do not need the full performance valued by customers at the high-end of the market. Figure 1 shows how Low-end enters the market and steals market share. New-market innovations target customers who have needs that were not previously served by existing technology, therefore creating a new market. Due to the nature of these innovations being less expensive and more creative in the services they provide, smaller firms can succeed in bringing them to market and stealing market share from larger firms.

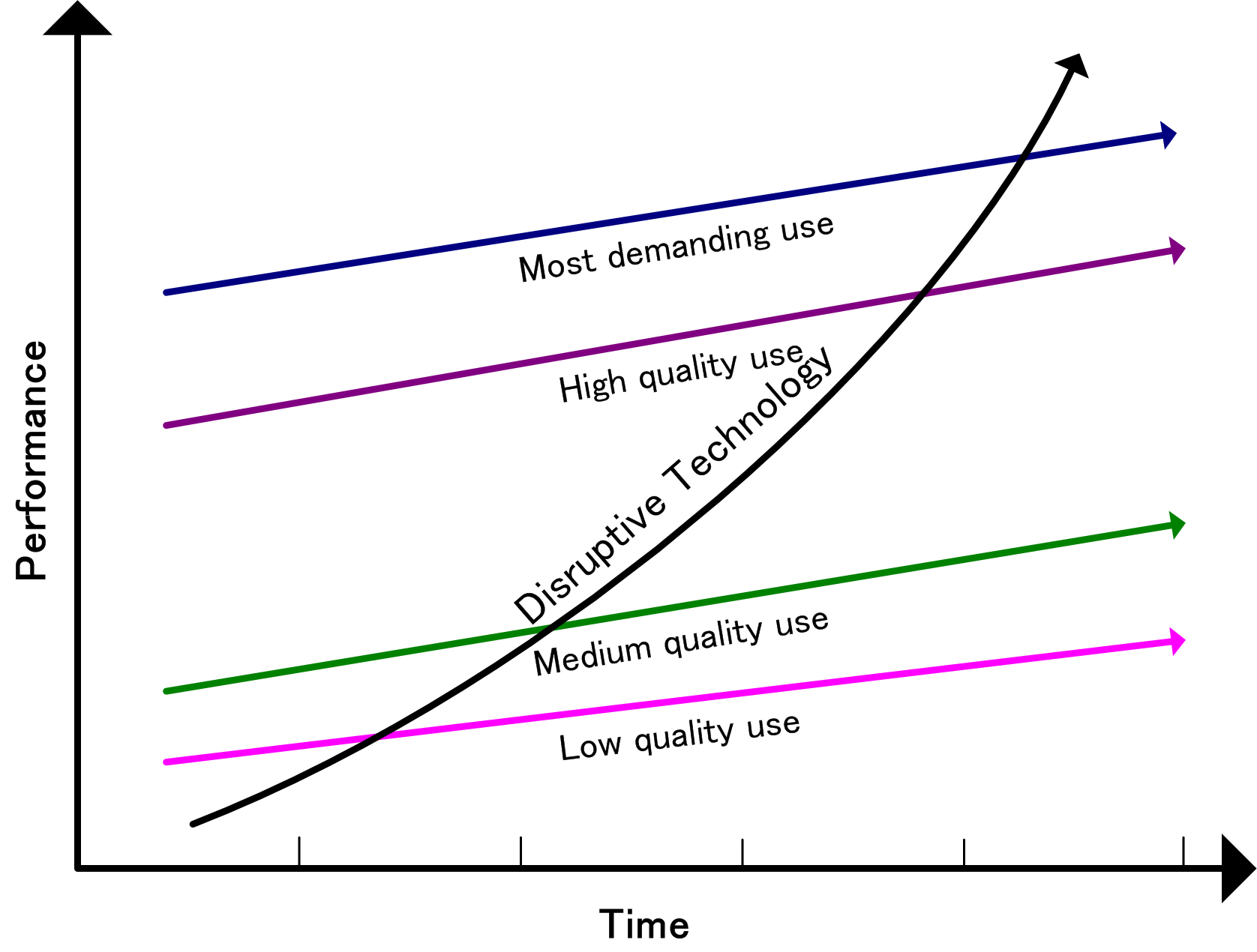


Figure 1. How a low-end disruptive innovation takes market share[[7]](#footnote-7)

The issue occurs when one considers exactly how this process will manifest in IoT. Large firms will bring clever technologies to market that offer some useful service. Over time, the cost of this service will decrease or the capability of the service will increase. In order to compete, small firms are incentivized to be more creative in the services they provide or offer more targeted, less expensive options. Essentially, they are forced to innovate.

Before long, every conceivable type of data will have an IoT device dedicated to collecting, analyzing, processing, and using it. As explained above, there may be 40 billion of them within five years. If these devices are not designed with privacy in mind, there may be consequences more significant that we can imagine. It is not sensationalism when we consider the fact that average technology consumers are now placing televisions with video cameras and gesture recognition in their bedrooms, nanny cameras and video-enabled Barbie dolls in their children’s rooms, microphones in the kitchen and living room, and a host of other sensors all over the house, and then connecting all of them to the Internet.

The other issue is the rate of innovation that these models suggest. When you consider exponential decrease in costs to producers, exponential growth in technology capability, and the incentive for small firms to bring disruptive technologies to market - the limit to human creativity is yet to be found - the outcome is rapid innovation. IoT technology will grow and develop more rapidly than any other in history. The issue is that regulation is, by design, slow moving and anchored. It takes time for new regulations and standards to take effect “due to the need to resolve tensions among divergent objectives of members of the private sector(s) and the state(s).”[[8]](#footnote-8) This “disparity in rates of change” is the issue that this paper intends to address by providing the key components of a planned adaptive approach to regulation.[[9]](#footnote-9)

## Motivation

There now exists a relatively new technology sector driven by IoT where it is fairly inexpensive and profitable to implement and innovate new ideas. With trillions of dollars in market share and billions of products within five years, it is no surprise that companies are clawing over each other to gain an edge. This technology sector also relies heavily on the collection, transportation, analysis, and understanding of data, much of which comes from individual users. Finally, the selling point of these consumer products hinges on an attempt to replace various delicate functions within the home or on the person.

The ultimate goal should be to capture the full potential of this new technology in a way the ultimately supports human value and the public interest. Figure 2 represents Sager’s Technology Integration coordinates and offers a useful tool for discussing the current state of a technology and determining its potential future paths. There is some argument as to the location of IoT technology in this model. Technology integration is certainly low, that much can be agreed. Considering the advertising buzz and market enthusiasm surrounding IoT, the technology seems to be in the “Grass Roots” sector. A few examples in this sector are cancer cures - high acceptance, just below average tech integration - and teleportation - high acceptance, extremely low tech integration. However, the 2015 Gartner Hype Cycle for Emerging Technologies shows IoT technology at the peak of inflated expectations, and therefore the hype surrounding that sector should be considered more cautiously.[[10]](#footnote-10) It is more likely that IoT technology is just within the “Emerging Market” sector due to the weak educational and regulatory efforts and the general misunderstanding of the technology and its standards for reasonable and appropriate use.[[11]](#footnote-11) A few examples of technologies in this sector are the Amazon delivery drones - just below average acceptance, just below average tech integration - and human cloning - low acceptance, low tech integration.

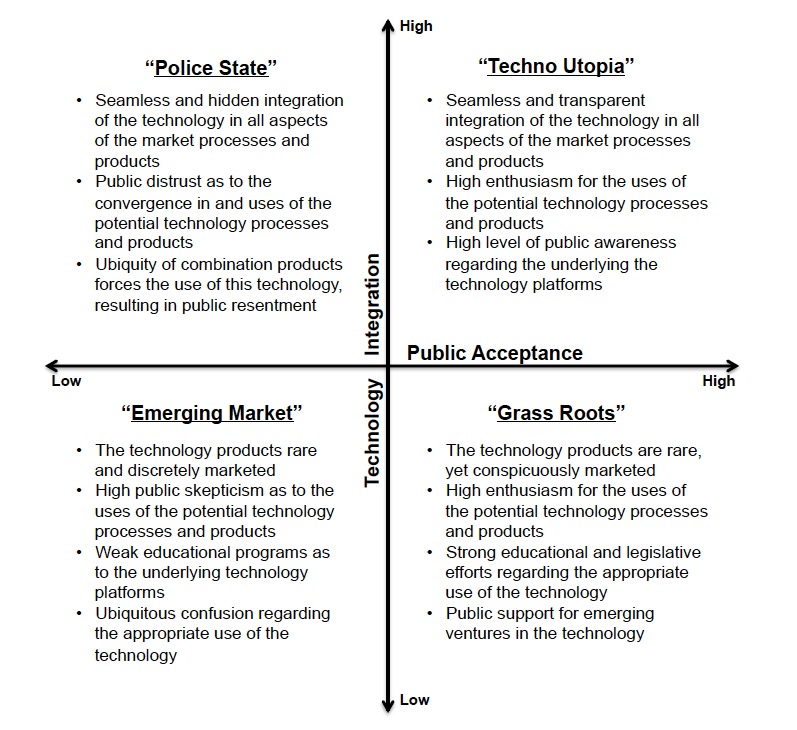


Figure 2. Sager's technology integration coordinates[[12]](#footnote-12)

The goal with for any significant technology is to enter the “Techno Utopia” sector and remain firmly entrenched. Technologies currently in this sector are automobile travel - high acceptance, high tech integration - and wind turbines - fairly high acceptance, fairly high tech integration. By extension, a technology does not want to enter the “Police State” sector. Once there, it becomes nearly impossible to leave. Further, the social and economic value of a new technology is greatly diminished once it is considered “Police State” tech.[[13]](#footnote-13) Examples of “Police State” technologies include traffic and speed cameras - low acceptance, high tech integration - and the NSA data gathering initiatives - fairly low acceptance, high tech integration.

The potential benefits of a large IoT market have already been shown. The goal, therefore, is to move IoT technology from the “Emerging Market” sector to the “Techno Utopia” sector. Both public acceptance and technology integration must be increased, but in a specific sequence. If technology integration were to be increased without public acceptance, IoT technology would find itself entrenched in the “Police State,” which is functionally impossible to leave. Therefore, public acceptance must be increased first in order to enter “Grass Roots” and then technology integration can be increased to enter “Techno Utopia.” The key factors of addressing public acceptance are: ethics, morality, cost, misunderstanding, fear, necessity, culture, political ideology, perceived pain of adoption, and regulation.[[14]](#footnote-14) By creating workable solutions for data privacy concerns with IoT products, nearly all of those factors will be addressed and public acceptance will be improved. This paper develops a framework to accomplish that.

Despite every device and service in this sector having published controlling documents, these policies all have similar inadequacies. Primarily, two basic inadequacies lead to data privacy concerns. First, there is a lack of technical standards and regulations within the space regarding data collection and usage leading to inconsistencies across different companies and products. Second, the Terms and Conditions and Privacy Policies of these documents often suffer from a lack of transparency with respect to what data is actually collected and how that data is used. These policies have a serious issue of clarity and scope. Companies do not clearly and concisely declare the types of data they collect and how that data is used. Companies also fail to regulate and limit their power and extent of ownership over the data. Without a sector-wide correction along these lines, the IoT industry may experience significant chilling effects or society may lose its sense and expectation of privacy.

This combination of factors is concerning. IoT products should not enter the market without some type of regulatory or standardized oversight. Regulators should consider establishing a structure for determining “data practices regarding collection, sharing, and use of IoT data.”[[15]](#footnote-15)At the dawn of the Internet, very few realized the future pervasiveness of that technology and the degree to which its implication would affect the world. Therefore, technical standards grew in isolation from value standards. In the case of the Internet, where the primary function is user communication, universal and early technical standards proved crucial to innovation and growth. However, IoT, as discussed earlier, is not just about communication. In the case of IoT, where the primary function is data collection and improving user efficiency and functionality, technical standards should be limited, marginal, and occur as needed. Conversely, value standards for the Internet of Things, due to the nature of user data privacy, must come early and be universal and complete. Additionally, some form of oversight is needed in order to ensure these devices and services, developed at a rate never before witnessed by humankind, support the goals of the consumers.

One can easily imagine the potential abuses by public and private actors these products draw into the home. Say, for example, the police are called to a home on a domestic abuse case. Upon arrival, they hear, through the door, an Amazon Echo. The Echo is a device that sits unnoticed in the corner of a room and is controlled entirely by your voice. It collects room state information including air temperature, air quality, number of people in the area, and can identify them based on voiceprint. A normal interaction would include asking the device to order you something from the Internet, play music, answer questions, and more, and all of this data is constantly streaming through wireless feeds to the cloud-based service. It also includes seven directional microphones and two-way audio, meaning a clever program could actually map the inside of a room down to the millimeter based purely on echolocation.[[16]](#footnote-16)

In all likelihood, the police could access this data and learn a great deal about the private details of one’s home without ever stepping foot inside. Then again, you may trust the law enforcement of the United States, or at least the legal system. Though this potential abuse of privacy is not limited to the confines of North America, that fact is beside the point. Let’s consider another entirely possible situation where our antagonist isn’t an officer of the law, but a thief, or a stalker, or perhaps even a murderer. Do we want them to potentially have access to that kind of data? Let’s also consider a less ominous situation where a company simply wants to know more about their configured users. Should they hear the private arguments between you and your spouse?

In terms of government abuse of these technologies, many precedents do exist that legally limit the potential for law enforcement privacy violations in the United States. In Kyllo v. United States (2001), the Supreme Court determined that law enforcement use of an electronic device without a warrant in order to gather state information about a private residence did constitute a search.[[17]](#footnote-17) In People v. Ramey (2009), exigent circumstances justified a warrantless search only in “an emergency situation requiring swift action to prevent imminent danger to life or serious damage to property, or to forestall the imminent escape of a suspect or destruction of evidence.”[[18]](#footnote-18) United States v. McConney (1984) further narrowed this definition by stating that a “reasonable person” must agree that the circumstances permit entry in order to “prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of a suspect.”[[19]](#footnote-19) The decision set forth in Riley v. California (2013) determined that “digital data ... cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee’s escape.”[[20]](#footnote-20) Horton v. California (1990) enumerates a three-part test for limiting plain view seizures: the officer must be lawfully present at the place where the evidence can be plainly viewed, the officer must have a lawful right to access the object, and the incriminating character of the object must be immediately apparent.[[21]](#footnote-21) And the declaration in Arizona v. Hicks (1987) that an “officer cannot move objects to get a better view” limits the definition of plain view.[[22]](#footnote-22) All of these cases and more - not to mention the 4th Amendment - provide significant limitations to privacy violations by the government in the United States.

These concerns, however, are not just in regards to privacy within the United States. They are also not just drawn in regards to a government’s violation of individual privacy. Companies and independent actors are also potential perpetrators of these violations. These companies and their devices and services are global and pervasive, as are their privacy concerns. This brand new technology, ripe for innovation, seeded for rapid growth and development, primed to explode in a market inundated with products that the configured users don’t even know they need, is charging headlong into risk. Without oversight, standardization, and review, these privacy concerns may bloom into privacy violations.

## Analytic Framework

There is a clear and pressing need for evaluating the privacy protections of IoT consumer devices. However, there is the issue that many of these devices have only existed for an exceedingly short period of time. Further, the technology and its operational concepts are new to everyone. All that currently exists are market and consumer projections. It is possible to gather insights from the Internet, and indeed we should, but that isn’t enough. The Internet serves fundamentally as a communication tool. IoT is a larger beast with what seem to be very large fangs. Therefore, in order to discuss how to go about protecting privacy in IoT, empirical data must actually be developed in order to analyze the privacy of IoT.

To find this data, I drew inspiration from a speech by Michael Crichton in 2008. Speaking on the topic of consensus science, global warming, and aliens (yes, aliens), he made the claim that “no longer are models judged by how well they reproduce data from the real world - increasingly, models provide the data. As if they were themselves a reality. And indeed they are, when we are projecting forward. There can be no observational data about the year 2100.”[[23]](#footnote-23) Therefore, I developed my own framework and my own data with which to “project forward” and provide a reality. Table 1 is a structured tool that can be used to assess privacy standards across the IoT consumer industry.

Table 1. Analytic framework for IoT products

|  |  |  |
| --- | --- | --- |
|  | Score | Weight |
| Readability | 0-3 | 2 |
| Accessibility | 0-3 | 2 |
| Scope | 0-3 | 3 |
| Moral Responsibility | 0-3 | 1 |
| User-defined privacy | 0-3 | 1 |
| Device-defined privacy | 0-3 | 2 |
| Data accessibility | 0-3 | 2 |
| User consent | 0-3 | 3 |
| **Total** | Sum of each Score multiplied by its Weight | |

### Measures for Analytic Framework

**Readability:** The degree to which the controlling documents are consumer-friendly in terms of ability to understand the details. Inversely related to amount of jargon/legalese

Metric: High (Score = 3), Average (Score = 2), Low (Score = 1), None (Score = 0)

**Accessibility:** The ease with which one may find and navigate the controlling documents in order to find desired information

Metric: High (Score = 3), Average (Score = 2), Low (Score = 1), None (Score = 0)

**Scope:** The degree to which the controlling documents limit the scope of a company’s ability to collect, store, and use various forms of data.

Metric: Limited (Score = 3), Average (Score = 2), Broad (Score = 1), Unstated (Score = 0)

**Moral Responsibility:** The degree to which the controlling documents include ethical language and address privacy concerns.

Metric: High (Score = 3), Average (Score = 2), Low (Score = 1), None (Score = 0)

**User-defined privacy:** The degree to which the company or device provides a mechanism for the user to actively manage or limit the extent and context of data collection.

Metric: High (Score = 3), Average (Score = 2), Low (Score = 1), None (Score = 0)

**Device-defined privacy:** The degree to which the obligation and application of data privacy rests on the engineering and structure of the product/service.

Metric: High (Score = 3), Average (Score = 2), Low (Score = 1), None (Score = 0)

**Data accessibility:** How easily data collected by the device/service may be accessed, amended, corrected, or eliminated by the user.

Metric: High (Score = 3), Average (Score = 2), Low (Score = 1), None (Score = 0)

**User consent:** The degree to which a device/service requires a user’s consent to store data, to alter policies, and to install software updates.

Metric: High (Score = 3), Average (Score = 2), Low (Score = 1), None (Score = 0)

### Explanation of Framework

Products with better privacy protections will receive a higher score (0-3) in each category. A weighting system (1-3) has also been implemented for each category, since certain measures are more essential than others. Most categories are weighted at “2” while necessary categories are weighted at “3” and less important categories are weighted at “1”.

These weights have been designed specifically with operational user data privacy in mind - operational in the sense that the consumer is actively using the device, and data privacy in the sense that the sensitive data within the area of operation is protected to the utmost. The ability of IoT products to collect sensitive data from a person’s home without some form of imposed limitation is the most concerning prospect with respect to privacy protection. That limitation may be self-imposed, due to government regulation, or as a function of technical standard setting. It is easy to abuse or misuse data beyond the purposes of the product. Thus, it is imperative that these products request user consent and limit the scope of their control over users’ data, hence the weight of “3” for those measures. While it is beneficial to a user when companies choose to use ethical arguments to address privacy concerns, it is not necessary for products with good privacy characteristics. Thus the weight of “1” for that measure. Additionally, companies should strive to design their products to be more aware of privacy responsibilities rather than putting that responsibility on the user. At the same time, the user should have some method with which they can further control the privacy settings of the IoT device. These facts account for that category’s inclusion in the framework as well as its low weighting.

While I have proposed an assignment of weights for this framework, these were drawn from my own logic for the goals of operational data privacy protection. I acknowledge that different goals may require different weightings and other groups who choose to use this tool can change the weights at their discretion.

As I will show, none of the most popular IoT devices scored “High” for all of the measures in the framework. In fact, most of the devices I analyzed scored “Low” in many of the measures. While this framework is easy to apply, the failures of current companies show that it sets a higher bar than most products currently meet today, which makes it a valuable tool to help improve privacy standards in the IoT consumer industry.

## Case Studies

In order to gain a better understanding of this technology space, I first conducted a series of case studies. The intent of these case studies was to gather empirical evidence regarding consumer data collection as well as to identify specific questions and areas of concern that might reveal trends. I initially looked at various IoT consumer devices that have received significant media attention in the past year and the devices found at “iotlist.co,” a website that specifically indexes IoT consumer products.

The criteria for further investigation were 1. the function of the product (I identified those devices with the highest potential for invasive use), 2. the types of data collected by the device (I specifically looked for devices that collect data with high information density such as video, sound, and environment information), and 3. the popularity of the devices. In the developmental process for the framework, full case studies were conducted on the following companies and products: Foscam baby-cam, Nest thermostat, Myfox, Netatmo, and Petcube. A series of similar questions regarding data collection and usage were identified from these case studies. These questions derived the eight measures of the evaluative framework. The framework was then applied to each product post hoc. The full case studies for all five products have not been included. However, in order to demonstrate how the products were analyzed and how the framework can be applied to products, I have included two representative examples: Myfox and Netatmo.

### I. Myfox[[24]](#footnote-24)

Myfox is a French company that offers a suite of devices for home security solutions. They offer a system, often bundled, that includes a home alarm, a control hub, window and door sensors called IntelliTAG™, and a surveillance camera. Their original patents were awarded in the early 2000s and by 2014 they had grown to 25,000 units installed with over 100,000 windows and doors secured by IntelliTAG™. The system itself claims to be the only alarm that alerts you prior to a break-in, which it accomplishes by using vibration sensors that can differentiate between innocuous activities, such as a knock, and potential threats, such as someone attempting to break a window. Further, the system also includes individual keychain identity tags that disarm the system when that specific key-fob enters the home. Finally, through the smartphone application, you can build a community that allows friends and neighbors certain access to the system. This access can in fact be tailored to each individual user with different permissions.

The most unique aspect of this camera is its mechanical privacy shutter. It is visibly obvious when this shutter is opened or closed and it can be programed to close or open when certain people are home, as identified by the key-fobs. The state of the shutter can be altered with the smartphone app provided the correct permissions are enabled for that user, and it automatically opens and begins recording when a break-in attempt is detected. The camera also includes two-way audio communications where you can hear as well as communicate through the device, as well as motion detection algorithms that trigger an alert when something “out of the ordinary” happens. As this device includes an obvious mechanism for users to tailor their privacy preferences, Myfox earns a “3” in User-defined privacy. The video recordings are entirely cloud-based with an optional subscription for up to seven-days of continuous recording space. The device does have some limited internal recording in case of a power outage or broken Wi-Fi connection, but the primary mode of video recording and transportation is through the cloud service. Further, the device is not designed to limit the amount of data sent to the cloud-based service. Therefore, Myfox earns a “1” in Device-defined privacy.

A telling aspect of the Myfox privacy policy is when they declare that by “using or visiting the Myfox website or mobile sites or applications provided by Myfox … you consent to our collection, storage, use, and disclosure of your personal information.” [[25]](#footnote-25) [[26]](#footnote-26) Myfox services collect quite a variety of personal information including your name, profile pictures from social media, location, gender, age and birthday, email address and account password, credit card details, customer support correspondence, technical and usage info including MAC address and IP address as well as log files for all connections, and location of device usage and room state information from all devices. Myfox declares that they “record and store archives of communications done through the service and done so on Myfox’s servers to protect the safety and wellbeing of our users and Myfox’s rights and property in connection with the service.” In this context “the service” refers to all actions taken in the operation and usage of Myfox devices. From this general description, and in conjunction with the technical details of the Myfox devices, it seems that Myfox collects and stores user data from all aspects of operation, which is made accessible through their cloud servers. They do provide a mechanism to access and amend this data, although it requires the user to contact Myfox directly and it is not clear whether that access is entirely complete. However, this still earns Myfox a “2” in Data Accessibility. In the context of the Readability and Accessibility measures, it should be fairly evident that Myfox succeeds in both and received a “3” in each. Despite the actual data-use concerns to be addressed later, the controlling documents themselves are exceedingly clear and navigable.

Myfox has published seven explicit uses and reasons for collecting and maintaining the right of use for user data. They are as follows:[[27]](#footnote-27)

1. *To create your accounts and allow use of our Service*
2. *To provide technical support and respond to user inquiries*
3. *To prevent fraud or potentially illegal activities, and enforce our Terms of Use*
4. *To deliver and target advertising*
5. *To notify users of updates*
6. *To solicit input and feedback to improve Myfox products and services and customize your user experience*
7. *To inform users about new products or promotional offers*

Further, they also publish their right to share information with Third-party Service (TPS) providers, such as call centers and fulfillment services, though only to provide services on Myfox’s behalf. These services include payment processing, data analysis, email delivery, hosting services, customer service, and marketing efforts. Site and platform operators such as “Amazon, Apple, Facebook, or Google may also collect or require that [Myfox] provides your information relating to the services.” To provide more specifics regarding one of these usages, Myfox may share user data in the form of aggregate or anonymous info as well as technical info like MAC addresses and mobile IDs for targeted advertising purposes.

While many of these data usage contexts seem to be framed in terms of advertising and user experience issues, the privacy policy does address more serious data concerns. They explicitly state the following:[[28]](#footnote-28)

*Your data, including without limitation chat text, voice communications, video, IP addresses, and your personal information, may be accessed and monitored as necessary to provide the Service and may be disclosed:*

1. *When we have a good faith belief that we are required to disclose the information in response to legal process (court order, search warrant, or subpoena)*
2. *To satisfy any applicable laws or regulations*
3. *Where we believe that the service is being used in the commission of a crime, including to report such criminal activity or to exchange information with other companies and organizations for the purposes of fraud protection and credit risk reduction*
4. *When we have good faith belief that there is an emergency that poses a threat to the health and/or safety of you, another person or the public generally*
5. *In order to protect the rights or property of Myfox, including to enforce Terms of Use*

The fact that Myfox’s servers collect such significant amounts of data, and that Myfox clearly declares that the data collected, including all video and voice communications, can be maintained and distributed at their discretion, is a bit disturbing. There is a clear cause for concern with this unparalleled access to extensive amounts of user data. For these reasons, Myfox has earned a “0” in Scope. Instead of limiting the scope to which Myfox can utilize private data, the policies seem to intentionally expand that scope.

At no point in the controlling documents does Myfox address the issue of receiving consent for data usage - they simply declare that by using the service, the user has granted complete consent. Nor do they mention or seem to be concerned with any ethical implications of their data collection and usage. In terms of notification of the user regarding changes in policy, Myfox has committed themselves to either “placing a notice on [the privacy policy], by sending you a notice to the e-mail address we have on file for you, or by placing notices on other Myfox websites.”[[29]](#footnote-29) However, considering the fact that additional consent is not required beyond simply purchasing the product, Myfox scores a “1” in User Consent. Additionally, Myfox scores a “0” in Moral Responsibility do to the fact that at no point in their controlling documents does the company seem concerned with ethical ramifications of their privacy characteristics.

Table 2. Analytical framework applied to Myfox products

|  |  |  |
| --- | --- | --- |
| **Myfox** | **Score** | **Weight** |
| Readability | 3 | **2** |
| Accessibility | 3 | **2** |
| Scope | 0 | **3** |
| Moral Responsibility | 0 | **1** |
| User-defined privacy | 3 | **1** |
| Device-defined privacy | 1 | **2** |
| Data accessibility | 2 | **2** |
| User consent | 1 | **3** |
| **Total** | 24 | |

According to the framework, Myfox scored 24 out of a maximum of 48, which is 50% privacy adequacy. The video surveillance device itself maintains a functional privacy safeguard in terms of the mechanical shutter, but that is clearly not enough to ensure the privacy of user data. It seems that the modus operandi of Myfox is to define all user data transmitted as in the public sphere and therefore usable as such. In this structure, the users are expected to provide their own safeguards by programming the device to maintain privacy.

### II. Netatmo[[30]](#footnote-30)

Netatmo is a French company founded in 2011 to develop consumer electronics specifically for a more connected and streamlined lifestyle. They opened their North American subsidiary in 2012. They currently offer three primary products: a thermostat (considered the French competitor to Nest), a weather/environment monitoring station, and Welcome. Welcome is their home security camera with built in facial recognition image processing software.

Welcome home security comes in the form of a tabletop camera and door/window tags. These devices communicate with a smart-device application that can be installed on all Apple and Android devices and can be accessed by anyone with the proper permissions and account authority. The camera itself comes with built-in facial recognition designed to inform users when specific individuals enter the field of view and communicates that info via the smart-device application. The device itself can maintain a profile on sixteen separate individuals. Within the application, a user can see who is currently home, a live stream of the video feed, as well as past events. A user can also customize each person’s privacy settings by disabling video recordings or notifications for individual people based on the camera’s ability to recognize those users. Due to this customization factor, Netatmo scores a “2” in User-defined Privacy. Further, the video data and identification information reportedly remains private by being stored within the camera itself on a local SD memory card. This structure provides a promising degree of Device-defined Privacy. However, screenshots of each major event (such as someone entering the feed) are stored for free in a cloud server for ease of access within the smart-device application. Additionally, when accessing the video feed from the application, the video data is sent through an end-to-end encrypted connection that can only be accessed with a Netatmo account and permissions. These factors all support the fact that Netatmo scores a “3” in Device-defined Privacy.

The terms of use[[31]](#footnote-31) are explicit about the expected users of these devices. In the first sentence they declare that anyone using the service must be at least 13 years old. Further, they also declare the exact types of information that the service involves, albeit they declare nearly every type of data: “software, text, graphics, communications, measures, tests, results, opinions, photographs, drawings, messages, notes, website links, music, video files, images, designs, music, audio files, reports, charts and data files.” The terminology used in the controlling documents is fairly common and easy to comprehend, earning Netatmo a “3” in Readability. However, they are somewhat frustrating to read. There is no obvious index or convenient way to navigate. Further, the clarity with which they address concerns such as data use and distribution, as well as user notification, is severely lacking. Therefore, Netatmo scores a “1” in Accessibility.

Within the terms of use and privacy policy, they actually state that the services rely entirely on user-generated content (UGC). Further, these documents are drawn around UGC and the rights you relinquish when using the service. First, you grant Netatmo an unlimited license to your UGC in all respects imaginable. Further, you “waive any rights of publicity and privacy with respect to the UGC and any other legal or moral rights that might preclude Netatmo’s use of the UGC or require your permission for Netatmo to use the UGC.” By defining the type of data involved in standard operations as every type of data, and then by declaring that they have irrevocable rights in all legal and moral respects to use that data, Netatmo draws a fairly ominous border around any expectation of data privacy. Netatmo provides literally no Scope to their collection and use of data, and therefore scores a “0” in that measure.

Further, possibly more surprising, the terms of use actually require the user to not develop any UGC that infringes on other’s rights or violates any law, as shown in the following clause:[[32]](#footnote-32)

*Your UGC:*

1. *Will not infringe any third party's copyright, patent, trademark, trade secret or other proprietary rights;*
2. *Will not violate any law, statute, ordinance or regulation;*
3. *Will not be obscene or contain child pornography;*
4. *Will not contain any viruses, worms, time bombs or other computer programming code that is intended to damage, detrimentally interfere with, surreptitiously intercept or expropriate any system, data or information;*
5. *Will not violate any third party's rights of publicity or privacy; and*
6. *Will not be defamatory, unlawfully threatening or harassing, harmful to minors in any way, or otherwise offensive or inappropriate. You are responsible for complying with all laws applicable to your UGC.*

Therefore, the user is entirely responsible to ensure that any data created by the usage of these devices does not violate those principles. This fact draws into limelight the issue of consent. Often, these devices are pointed at a door that, when opened, reveals a much larger world with many events within the frame of video recording. This clause technically addresses some ethical privacy concerns, but not in the way we would expect. Instead of concerning themselves with the ethical privacy of their users, Netatmo requires the users to consider the ethical implications of their use of the service. These concerns are certainly important in terms of privacy rights and protections, but not typically the types of concerns one would expect a policy to address. Therefore, they score a “2” in Moral Responsibility.

The privacy policy does make note of various requirements. For example, collection and processing of all personal data adheres to the French law 78-17 of 6 January 1978 regarding data privacy. Further, Netatmo clearly states, “You have the right to access, amend, correct and eliminate data concerning you at any time.”[[33]](#footnote-33) That request must be sent by physical post to an office in France – a certain barrier to invoking that right. Therefore, Netatmo scores a “1” in Data Accessibility. A user should not incur a cost to invoke a sub-function of their right to privacy. Similarly, Netatmo provides minimal evidence that it will practice effective User Consent. The Terms of Use does declare that a user must “provide prior written consent before we use certain types of cookies.” However, Netatmo also “reserves the right to update or modify this Privacy Policy at any time and from time to time without prior notice.”[[34]](#footnote-34) This fact suggests that User Consent is not a priority to Netatmo, earning them a “1” in that measure.

Table 3. Analytic framework applied to Netatmo products

|  |  |  |
| --- | --- | --- |
| **Netatmo** | **Score** | **Weight** |
| Readability | 3 | **2** |
| Accessibility | 1 | **2** |
| Scope | 0 | **3** |
| Moral Responsibility | 2 | **1** |
| User-defined privacy | 2 | **1** |
| Device-defined privacy | 3 | **2** |
| Data accessibility | 1 | **2** |
| User consent | 1 | **3** |
| **Total** | 23 | |

According to the framework, Netatmo scored 23 out of a maximum of 48, which is 47.92% privacy adequacy. It is interesting to note the difference between Netatmo’s approach to data privacy and Myfox’s. Both offer comparable services with somewhat different approaches to data concerns. Myfox utilizes a mechanical form of privacy protection in their camera shutter with all collected data sent to a central cloud storage system that the company may access. Therefore, it is up to the user to determine when more privacy is required. Netatmo on the other hand does not send any video data to the cloud. Instead, all video is maintained locally and cannot be easily accessed by the company. Other information such as screenshots and identification and location data is stored in the cloud, but video itself is not. Therefore, the device determines a certain degree of privacy regardless of user intent.

## Discussion

Table 4. Example of the analytic framework applied to a market of five products

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Foscam** | **Nest** | **Myfox** | **Netatmo** | **Petcube** | **Market Totals** |
| Readability (2) | 2 | 3 | 3 | 3 | 3 | **28/30 = 93.3%** |
| Accessibility (2) | 1 | 3 | 3 | 1 | 2 | **20/30 = 66.7%** |
| Scope (3) | 1 | 2 | 0 | 0 | 1 | **12/45 = 26.7%** |
| Moral Responsibility (1) | 0 | 3 | 0 | 2 | 3 | **8/15 = 53.3%** |
| User-defined privacy (1) | 1 | 1 | 3 | 2 | 3 | **10/15 = 66.7%** |
| Device-defined privacy (2) | 1 | 2 | 1 | 3 | 1 | **16/30 = 53.3%** |
| Data accessibility (2) | 0 | 2 | 2 | 1 | 0 | **10/30 = 33.3%** |
| User consent (3) | 1 | 2 | 1 | 1 | 1 | **12/45 = 26.7%** |
| **Total** | **15/48 = 31.3%** | **32/48 = 66.7%** | **24/48 = 50.0%** | **23/48 = 47.9%** | **24/48 = 50.0%** |  |

Table 4 shows the results of five complete case studies for various IoT consumer products. Other detailed studies have not yet been completed. However, less formal reviews have also been completed for popular IoT products such as Neurio, FitBit, and Amazon Echo. Throughout these reviews and case studies, a few clear trends have emerged. The last column in Table 3 shows market totals for each measure - the market in this case being these five products. Any total greater than 60% should be considered acceptable in the current state of this technology sector. Any total greater than 80% should be considered good, and any total greater than 90% should be considered excellent. Naturally, the goal is to achieve 100% in every category, and the market should strive to do so.

To start with the promising trends, the Readability of the controlling documents in this market is extraordinarily good. This fact suggests that companies do make some attempt at ensuring their controlling documents are understandable to the configured users. Keep in mind, the only content issue covered by Readability is the degree to which the company’s documents rely on legalese. Therefore, while this high score does not say anything about privacy protections themselves, it represents success in a crucial step of privacy protection and part of applying planned adaptation – consumer buy-in – to be discussed later. By making these documents readable, companies ensure that those people who are interested in gaining a deeper understanding of the product and services may do so, a promising implication.

Accessibility and User-defined Privacy also have relatively high market scores. Again, these measures support consumer buy-in, a crucial aspect of privacy protection. By making the controlling documents and details regarding personal data relatively accessible, consumers may review how a company conducts its service as a kind of pre-operational protection. On the other end, User-defined Privacy allows for the consumer to tailor their use of the device to gain some semblance of operational privacy. Both practices are key parts of gaining consumer buy-in and it is quite promising that the market already scores high in these areas.

Disturbingly, the two most important measures, Scope and User Consent, have the lowest market scores. I have defined my use of this framework and the weighting matrix in order to best support the goal of user data privacy in the home. A number of subjective factors led to the weighting matrix, but it has thus far worked consistently as applied. Scope and User Consent are the two most important ways in which a company can prove to the consumer that they take data privacy seriously. Scope shows the consumer that the company is willing to self-regulate their invasive services. User Consent shows the consumer that the company respects their own individual privacy desires and is willing to tailor the service to some degree. It is a bit disconcerting that these measures have such low market totals because it shows that IoT companies do not respect the privacy desires of their users. Given these concerns, our attention should be drawn to this specific focus in order to encourage innovation and change.

## Planned Adaptation

The planned adaptive approach to technology policy and regulation is an attractive one, especially in inherently dynamic fields. The term implies a sense of pliability, or perhaps even evolution. Just as in biology, where a species prone to adaptation is best suited to survive, so it seems planned adaptive regulation may be the most effective approach in a changing world. There are three traits inherent to any adaptive system, as defined by a control systems engineering approach. There is the observation of a system dynamic, the measurement of the dynamic, and the subsequent control signal. It is important to note that many assume that some form of feedback is inherent to this system. However, some of the most effective control systems are actually built with feedforward loops as opposed to feedback loops. Both of these concepts are crucial to the potential effectiveness of planned adaptation.

Feedforward control takes an output of a system and applies it in a predetermined way. Feedback control takes an output of a system and alters the system control based on that output. Feedforward loops are often used in extremely dynamic processes such as drone control and automation in robotics, as well as a host of natural applications. For example, in physiology there is an anticipatory regulation of the human heartbeat prior to a physical exertion. Another form of natural feedforward control is in gene regulation and transcription factors. When a gene detects a non-temporary environmental change, gene A will activate gene B, and gene A and B will together activate gene C. We can draw specific conclusions about feedforward, which is that it is a learned anticipatory response to specifically defined cues and it is inherently fast. Conversely, feedback regulation can provide further adjustment and precise adaptation, but it is cumbersome and more time consuming - just like the regulatory process in the United States.

As previously shown, the IoT environment shows an inherent character of rapid innovation. It is a fast process. Meanwhile, the regulatory environment shows an inherent character of glacial rates-of-change. It is a slow process. It is important to note that there is nothing inherently wrong with a slow regulatory process. Again drawing a metaphor from control systems engineering, controls on a system have the effect of damping its response. An undamped system will perpetuate its response regardless of that output. In this space, that means no regulation or standardization, and therefore no control. A damped system has some form of control, but the implementation becomes tricky. If the goal is to have rapid control in a fast moving system, the control will be underdamped. Sometimes underdamped is good and, when well designed, will lead to the desired system response. However, if poorly designed, underdamped control will lead to an unstable response and the system will tear itself apart. The final type of control is heavy and cumbersome and called overdamped. In this case, the system will respond slowly, but it is fairly predictable in its response. Regulation, as a form of system control, follows these natural laws.

In a recent paper, Dr. David Clark discussed the improbability of the planned adaptive approach to system control working in the information and communication technology (ICT) environment. His argument was founded in the same control systems approach I outlined above. He concluded that the “disparity in rates of change” between technology innovation and government processes would result in four possible scenarios:[[35]](#footnote-35)

1. *Industry constantly out-evolves the controls of the state.*
2. *The pace of evolution (industrial innovation) slows, perhaps by explicit government intervention, to the rate at which the state can evolve its laws and regulation.*
3. *The pace of evolution in regulation speeds up to match the pace of technical evolution.*
4. *Regulators anchor policies around stable points in the system architecture.*

Scenario one is essentially an undamped and uncontrolled system. Scenario two is an overdamped, heavily controlled and regulated system. Scenario three is an underdamped system with engineered regulation that can result in instability. Scenario four is actually a feedforward method of control, and Dr. Clark’s central claim as the proper regulatory framework for the ICT environment.

These details matter because many assume planned adaptation fits solely within the realm of underdamped control and is therefore prone to instability (scenario three). However, the framework I have proposed can be used in a planned adaptive approach as both underdamped feedback control as well as anchored feedforward control - scenarios three and four respectively - and can be successful in both forms depending on how it is applied.

As a form of underdamped feedback control in the IoT realm, there are five requirements and process stages that must be met.[[36]](#footnote-36) These stages are drawn from the same work on ICT policy development that addressed the disparity in rates of change above. First, there must be an agreement on the policy goals. Second, there must be a definable way to empirically measure progress toward that goal. Third, regulatory options must be specifically designed to support those goals. Fourth, analysis must be conducted to show that the new policies and regulations were actually a causing factor in the system response. Finally, there should be a system to observe and address possible destabilization or unintended consequences from those policies and regulations.

The framework introduced, designed, and applied earlier in this paper directly addresses and supports the first three stages in this process. In its current form of eight measures and the weighting matrix, the analytic framework specifically engages the policy goal of increasing consumer data privacy. Dr. Clark makes a clear argument for the specification of goals and outcomes as opposed to the specification of rules. Outcome specifications are higher level, more representative of ethical values, and create a target area for the regulation. In other words, they provide for more flexibility in the creation and application of the actual regulations to address the goal. The framework is currently drawn to address data privacy. It could also be drawn to support the goals of data security, user experience, market efficiency, and product functionality, and probably more. Therefore, the first necessary stage to implementing adaptive regulation is well met, both functionally and with flexibility, by the analytic framework.

The framework also addresses the second stage, the ability to actually measure progress towards those goals. As was shown in the framework section, the structure of the measures, metrics, and their weights provide clearly drawn data. Theoretically, if every IoT consumer product in the market has undergone that analysis, the ability to measure specific goals is extensive. One could look at the market totals for each category to determine which measures are lagging, or subsets of the market such as video devices or utility-monitoring devices could be analyzed to determine more specific measurements. Further, companies could look at the results of their entire catalog in order to target areas for innovation and development. The framework provides extensive amounts of data; the only limitation is the creativity of those who determine what to do with it.

This function of the framework also touches on the third stage of applying planned adaptive regulations to IoT. Under this requirement, regulatory choices must be narrowly drawn in order to address the specific goals. The framework provides that focus. Take, for example, the five-product market demonstrated earlier in this paper. Scope and User Consent were particularly low among those products. Therefore, it is now known that in order to move the entire system toward the goal of data privacy, regulatory actions must be drawn in order to address those specific measures. Further, we can monitor the progress of that goal based on archived data and the rate of change for each measure.

The final two requirements for applying a planned adaptive architecture have more to do with the structure of the regulatory authority than the three directly addressed by the framework. One regards proving causality between the regulation and the market improvement towards the goal. That function is a statistics issue and a matter of applying known principles. Granted, the structure must provide for this requirement, but it is not a limiting factor to its application. The last requirement might be limiting. It regards the potential instability created by rapidly changing regulation as the main argument for why planned adaptation will not work for IoT. Every other requirement has been met. In order to solve the potential issue of instability, a feedforward system should also be included in the application of a planned adaptive approach to IoT regulation.

The primary issue to address is how exactly to apply the framework in a way that ensures feedforward control. Again, feedforward control is inherently adaptive and allows for the system dynamics to function relatively unimpeded. Instead of altering the inputs to the system based on a regulator - this would be the technology in the IoT market - feedforward control is used to determine exactly how the system interacts with those inputs. If we intelligently design an application of the framework to inform the system, the IoT market, of the goals and measurements made through the feedback system, feedforward control should take hold. The inspiration for this additive approach comes from Dwight D. Eisenhower’s farewell address to the nation on January 17, 1961 when he said the following:

*In the councils of government, we must guard against the acquisition of unwarranted influence, whether sought or unsought, by the military-industrial complex. The potential for the disastrous rise of misplaced power exists and will persist. We must never let the weight of this combination endanger our liberties or democratic processes. We should take nothing for granted. Only an alert and knowledgeable citizenry can compel the proper meshing of the huge industrial and military machinery of defense with our peaceful methods and goals, so that security and liberty may prosper together.[[37]](#footnote-37)*

While Eisenhower was specifically discussing the potential for tyranny granted by the military-industrial complex of the mid-20th century, there are parallels to be drawn today. We now have an information technology complex with a similar potential for tyranny or abuse of privacy, at the very least. The solution that Eisenhower presented, an “alert and knowledgeable citizenry” remains valid. By applying the framework in two concrete and distinct formats with well-defined parameters, we can design a feedforward method of control that improves any planned adaptive approach.

The first method involves the use of labeling. Labeling is a well-established practice for risk mitigation, and relies primarily on the classification of the issue, risk, or goal one is trying to solve. As Granger Morgan shows in his theory of risk shielding, when the risks of a technology are not particularly observable or well defined, yet the effects are controllable, then labeling is often a functional approach to risk shielding.[[38]](#footnote-38) Similar examples include over-the-counter medication, hazardous materials, and food supplements. Looking once more to the framework with labeling in mind, it already resembles the nutritional facts found on any processed food item. By adding this label to products, one could predict the actions of people and the effects on the market. Specific groups of people would have their own weighting matrices for the measures that would determine their purchasing actions. Again, these are all measurable effects with predictable outcomes. It is a feedforward method of control due to this predictability. The labels don’t change, nor do they necessarily affect the method of regulatory control, they directly affect the system itself. Therefore, it minimizes any potential for instability.

The second method applies more directly to the planned adaptive regulatory approach. It involves the use of open invitations for input, public consultations, and review of potential regulations. Most importantly, it has already been proven to work in the ICT realm. In 2009, during the lead up to drafting Brazil’s Internet law, the Marco Civil da Internet, the Brazilian Ministry of Justice launched a special review task force. The law itself was to cover issues such as net neutrality, privacy, security, and more. This group was charged with collecting public comments and consulting self-defined interest groups regarding the potential law.[[39]](#footnote-39) These considerations were able to identify, by design, the stakeholders in the regulation. Further, the task force was able to compile a meaningful study regarding various suggestions and input from individual citizens, companies, and groups.[[40]](#footnote-40) The Ministry of Justice then drafted the law, and released it again to the same task force to gather additional public input. Once all the input was analyzed, and the draft was amended to reflect the public interest, only then was the bill written and signed into law in 2014. This process took five years start to finish.

The same approach can be applied to IoT privacy issues. This process implements a form of feedforward control that can help mitigate the instability caused by rapid regulatory change. The data being fed forward is the direct, measured input from the stakeholders in the system. Simply by measuring this data set, the system is altered directly by increasing the interest and buy-in of the stakeholders. This form of transparency allows for the system inputs to adjust themselves accordingly despite the knowledge of future regulation because they can predict the outcome. Further, this process utilizes a feedback loop when the data is then used in a predictable way to actually design or alter the system control, the regulation. Therefore, feedback and feedforward are used in conjunction to maximize control and minimize instability.

Putting it all together, the analytic framework provides the necessary perspective and data to articulate goals as well as design and apply regulation to IoT. Regulators should apply the framework in order to maintain a complete view of the IoT market. For example, the FTC could appoint a review board to apply the framework to new consumer products as they enter the market. This way, the empirical data needed to target regulation would be readily available. The framework should also be applied as a labeling tool for consumer products. The market forces will then pick winners and losers and influence the rapid development of technologies based on consumer interests. Finally, a full market review that includes the solicitation of input from stakeholders will provide the necessary knowledge foundation prior to actually designing further regulation. These reviews should be triggered by trends in the framework dataset from the IoT market. For example, when the market total for one of the key measures, such as Scope or User Consent, falls below a certain percentage – 60% should work well – this fact would trigger further investigation and a review for renewed regulation. It is also possible to define other goals and triggers that would be equally as effective in triggering regulatory review. This way, we can design a truly adaptive regulatory structure for the IoT environment that also maintains stability.

## Conclusion

While it is clear that IoT technology offers a magnitude of potential economic and social benefits, the perpetuity with which these devices collect sensitive data is an area of serious concern. User data privacy must be taken more seriously by the companies building and innovating these products, by the configured users who create the market demand, and by the governments who care about human value. The first steps in this process require actually measuring the technology, determining how products apply privacy principles, and collecting usable data for evaluating privacy goals. The evaluative framework designed and implemented in this paper accomplishes these steps. Next, that same framework must be functionally applied to the IoT space in order to create awareness and foster improvement. All consumer technologies and products entering the market should undergo the framework analysis. Further, the framework should be transformed into a type of product label. That way, it will be possible to measure the privacy protections of the products on the market. It will also improve the consumers’ understanding and awareness of the technology’s usage implications. Finally, that host of data can be designed in a way to trigger more significant regulatory reviews in a multi-stakeholder process designed to minimize the destabilizing effects of adaptive regulation.

# Works Cited

1. *Arizona v. Hicks.* 85-1027 (United States Supreme Court, March 3, 1987).
2. Castillo, Andrea, and Adam Thierer. *Projecting the Growth and Economic Impact of the Internet of Things.* Market Report, Mercatus Center, George Mason University, Arlington, VA: Mercatus Center, 2014.
3. Clark, David C., and K.C. Claffy. "Anchoring policy development around stable points: an approach to regulating the co-evolving ICT ecosystem." *Telecommunications Policy* (Center for Applied Internet Data Analysis) 39, no. 39 (2015): 848-860.
4. Crichton, Michael. "Aliens Cause Global Warming." *The Wall Street Journal*, November 7, 2008.
5. Eisenhower, Dwight D. *Farewell Address to the Nation.* January 17, 1961.
6. Felsberg Advogados. "Brazil launches consultations on internet and privacy laws." *Felsberg Advogados.* September 3, 2015. http://www.felsberg.com.br/en/brazil-launches-consultations-on-internet-and-privacy-laws/ (accessed December 1, 2015).
7. Gartner. *Gartner's 2015 Hype Cycle for Emerging Technologies.* August 18, 2015. https://www.gartner.com/newsroom/id/3114217 (accessed December 1, 2015).
8. Gatto, Raquel. "The Brazilian Experience of Public Consultation for the “Marco Civil Da Internet” and The Data Protection Law." *Internet Society.* February 3, 2015. The Brazilian Experience of Public Consultation for the “Marco Civil Da Internet” and The Data Protection Law (accessed December 1, 2015).
9. *Horton v. California.* 88-7164 (United States Supreme Court, June 4, 1990).
10. Iron Paper. *Internet of Things Market Statistics - 2015.* March 5, 2015. http://www.ironpaper.com/webintel/articles/internet-things-market-statistics-2015/ (accessed October 1, 2015).
11. *Kyllo v. United States.* 99-8508 (United States Supreme Court, June 11, 2001).
12. Manyika, J, M Chui, P Bisson, J Woetzel, R Dobbs, and J Bughin. *The Internet of Things: Mapping the Value Beyond the Hype.* Market Study, McKinsey Global Institute, McKinsey & Company, McKinsey & Company, 2015.
13. Morgan, M. Granger. "Risk Analysis and Management." *Scientific American*, July 1993: 24-30.
14. Myfox. *Myfox Smart Home Security Solutions.* October 1, 2015. http://www.getmyfox.com/ (accessed October 1, 2015).
15. —. "Privacy Policy." *Myfox Home Security Solutions.* January 4, 2015. http://www.getmyfox.com/us\_en/privacy-policy.html/ (accessed October 1, 2015).
16. —. "Terms of Use." *Myfox Home Security Solutions.* January 4th, 2015. http://www.getmyfox.com/us\_en/terms-of-use.html/ (accessed October 1, 2015).
17. Netatmo. *Netatmo Home Security.* October 1, 2015. https://www.netatmo.com/ (accessed October 1, 2015).
18. —. "Terms of Use." *Netatmo Home Security.* January 30, 2012. https://www.netatmo.com/zh-TW/site/terms (accessed October 1, 2015).
19. Peckham, Matt. *We Can Now Map Rooms Down to the Millimeter with a Finger Snap.* June 19, 2013. http://techland.time.com/2013/06/19/we-can-now-map-rooms-down-to-the-millimeter-with-a-finger-snap/ (accessed December 1, 2015).
20. *People v. Ramey.* 1-07-2217 (Appellate Court of Illinois, First District, First Division, August 10, 2009).
21. Raysman, Richard. *Enforceability of Clickwrap Agreement Called into Question.* November 7, 2012. http://www.hklaw.com/digitaltechblog/Enforceability-of-Clickwrap-Agreement-Called-into-Question----Checklist-for-Best-Practices-in-Electronic-Contracting-11-07-2012/ (accessed November 20, 2015).
22. *Riley v. California.* 13-132, 13-212 (United States Supreme Court, June 25, 2014).
23. Rinesi, Marcelo. "The price of the Internet of Things will be a vague dread of a malicious world." *Institute for Ethics and Emerging Technologies.* September 25, 2015. http://ieet.org/index.php/IEET/more/rinesi20150925 (accessed October 1, 2015).
24. Sager, Brian. "Scenarios on the future of biotechnology." *Technological Forecasting and Social Change* (North Holland) 68 (2001): 109-129.
25. Smith, Aaron. "What Internet Users Know about Technology and the Web." Market Study, Internet, Science, and Technology, The Pew Research Center, 2014.
26. *United States v. McConney.* 80-1012 (United States Court of Appeals, Ninth Circuit, June 15, 1982).
27. Wikipedia. "Disruptive Innovation." *Wikimedia.* October 18, 2005. https://upload.wikimedia.org/wikipedia/commons/c/c4/Disruptivetechnology.png (accessed November 30, 2015).

1. (Smith 2014) [↑](#footnote-ref-1)
2. (Iron Paper 2015) [↑](#footnote-ref-2)
3. (Castillo and Thierer 2014) [↑](#footnote-ref-3)
4. (Ibid) [↑](#footnote-ref-4)
5. (Manyika, et al. 2015) [↑](#footnote-ref-5)
6. (Castillo and Thierer 2014) [↑](#footnote-ref-6)
7. (Wikipedia 2005) [↑](#footnote-ref-7)
8. (Clark and Claffy 2015) [↑](#footnote-ref-8)
9. (Ibid) [↑](#footnote-ref-9)
10. (Gartner 2015) [↑](#footnote-ref-10)
11. (Rinesi 2015) [↑](#footnote-ref-11)
12. (Sager 2001) [↑](#footnote-ref-12)
13. (Sager 2001) [↑](#footnote-ref-13)
14. (Ibid) [↑](#footnote-ref-14)
15. (Manyika, et al. 2015) [↑](#footnote-ref-15)
16. (Peckham 2013) [↑](#footnote-ref-16)
17. (Kyllo v. United States 2001) [↑](#footnote-ref-17)
18. (People v. Ramey 2009) [↑](#footnote-ref-18)
19. (United States v. McConney 1982) [↑](#footnote-ref-19)
20. (Riley v. California 2014) [↑](#footnote-ref-20)
21. (Horton v. California 1990) [↑](#footnote-ref-21)
22. (Arizona v. Hicks 1987) [↑](#footnote-ref-22)
23. (Crichton 2008) [↑](#footnote-ref-23)
24. (Myfox 2015) [↑](#footnote-ref-24)
25. (Myfox 2015) [↑](#footnote-ref-25)
26. (Ibid) [↑](#footnote-ref-26)
27. (Ibid) [↑](#footnote-ref-27)
28. (Myfox 2015) [↑](#footnote-ref-28)
29. (Myfox 2015) [↑](#footnote-ref-29)
30. (Netatmo 2015) [↑](#footnote-ref-30)
31. (Netatmo 2012) [↑](#footnote-ref-31)
32. (Ibid) [↑](#footnote-ref-32)
33. (Netatmo 2012) [↑](#footnote-ref-33)
34. (Ibid) [↑](#footnote-ref-34)
35. (Clark and Claffy 2015) [↑](#footnote-ref-35)
36. (Clark and Claffy 2015) [↑](#footnote-ref-36)
37. (Eisenhower 1961) [↑](#footnote-ref-37)
38. (Morgan 1993) [↑](#footnote-ref-38)
39. (Felsberg Advogados 2015) [↑](#footnote-ref-39)
40. (Gatto 2015) [↑](#footnote-ref-40)