Literature Review:

Raising Consumer Awareness and Security for Internet of Things Devices

English 316 Technical Communications, Section 024

Nathaniel Wilson

Abstract

The internet of things has ushered in a new wave of devices which handle and generate personal data at an unprecedented rate. Personal data managing technology has brought immense benefits, along with new risks and problems with consumer security. IoT devices give digital sources access to aspects of consumers’ physical worlds and digital information. These integrated and widespread applications bring into question the risk-to-benefit cost for consumers and how well the device manufacturers ensure the protection of their privacy. While the IoT is still early in development, it is critical that adopters of its technology are educated and understand the risks and responsibilities that come with integrating the internet into their lives. To increase awareness, I propose a consumer minded label to present basic security and data management information, allowing them to make well informed decisions.

[Introduction 4](#_Toc501720024)

[Analysis of Field and Issue 5](#_Toc501720025)

[Overview of Personal Data Security 5](#_Toc501720026)

[Overview of the Internet of Things 6](#_Toc501720027)

[Industry Standards for Consumer Privacy 7](#_Toc501720028)

[Consumer Privacy Enforcement by the FTC 7](#_Toc501720029)

[Compromises to Consumer Privacy Standards 8](#_Toc501720030)

[TRENDnet Webcams 9](#_Toc501720031)

[Mirai 9](#_Toc501720032)

[Current Consumer Awareness of Security Risks 10](#_Toc501720033)

[Proposed Solution 11](#_Toc501720034)

[Description 11](#_Toc501720035)

[Improving Data Security 12](#_Toc501720036)

[Example Mock-Up 13](#_Toc501720037)

[Required Permissions 13](#_Toc501720038)

[Secure Device Procedures 13](#_Toc501720039)

[Opt-In Permissions 14](#_Toc501720040)

[Anticipated Results 14](#_Toc501720041)

[Suggested Further Research 14](#_Toc501720042)

[Conclusion 14](#_Toc501720043)

[References 16](#_Toc501720044)

# Introduction

In modern society, Internet technology has been integrated into our lives so much, that our day-to-day activities depend on its infrastructure. As computers and access to the internet have become more widely available, so has the importance of the digital world. Communication, entertainment, financial transactions, and data storage all occur between the digital devices we use to connect with each other. Until recently, the internet’s influence was restricted to interacting within this digital world, but now the internet is increasingly connected and responsive to the physical world, through internet enabled devices.

These devices are what comprise the “Internet of Things” or “IoT.” No longer does the internet just connect personal computers; it now connects televisions, smart phones, thermostats, health monitors, and even cars, to the world wide web. This development hasn’t come about just to provide new toys and sleek smart devices to tech enthusiasts. By connecting devices to the internet, industries have been able to automate factories, provide incredibly accurate and useful real-time data, and, ultimately improve and ensure coordination between digital and physical systems. Industries have a lot to gain from using IoT devices where timely data validation is money.

But what does the average consumer have to gain by using IoT devices? Is it added security or ease for having a blue-tooth enabled door lock, or a systems that keep track of their physical life using digital systems? Or is it the surveillance of easy to use indoor wi-fi security camera system? Companies such as Amazon, Google, and Apple have invested in consumer IoT devices as a growth industry. From home hubs such as the Amazon Alexa, to wearable technology like the Fitbit, these devices provide users with interactive and automated systems.

The flip-side of relying on internet technology, especially IoT devices, are the privacy and security vulnerabilities. IoT devices give digital sources access to aspects of one’s physical world as well as one’s digital information. While the IoT is still early in development, it is critical that adopters of its technology are educated and understand the risks and responsibilities that come with integrating the internet into their lives.

Section one will cover the topics surrounding the issues of consumer privacy and security. Several devices and instances of data vulnerabilities will be studied to determine underlying trends in the industry. Then I will give a brief analysis on the consumer response and awareness to these vulnerabilities

Section two will cover the proposed solution and its methodology. Part of the solution will be analyzing other solutions to the same problem in different settings. I will then present my example of an informing customer label followed by a brief section will cover the anticipated results of its implementation.

# Analysis of Field and Issue

## Overview of Personal Data Security

Modern society requires that every individual has information about themselves stored and routinely used. Governments and private businesses often require several forms of key identifying information to use their services. This information includes simple alpha-numeric sequences such as Social Security numbers, birthdates, names, methods of payment, addresses, and phone numbers. This information ties us to rights of ownership, residence, and records; therefore, we need to be selective with how we distribute that info.

Before digitization, for institutions, such as hospitals or banks, privacy was clear because personal data and records only existed in one place at a time. The line was blurred when digital records became more viable and reasonable for businesses to keep. Digital files were still relatively private because they could only be accessed within the institutions’ database. With the advent of the internet, online file sharing made transitions between locations and institutions seamless. However, internet connectivity also gave access to malicious cyber criminals and, in some instances the ability to hijack private information.

At the formation of the commercially viable internet, the FTC released a statement about research on consumers’ concerns about online data security. “Consumers have less confidence in how online service providers and merchants handle personal information than they have in how traditionally offline institutions, such as hospitals and banks, handle such information.” (FTC, 1998, 3) This initial hesitancy did not hold up. Within two years the FCC reported that “data suggest that consumers spent as much as $2.8 billion online during the month of January 2000 alone.” (FTC, 2000, pg.2) The trade-off between risk and benefit ultimately payed off as participation in the online market skyrocketed.

Nearly two decades later, online transactions have become the norm, so it is no surprise that new internet enabled devices do not raise the same red flags as they did back in the early days of the commercial internet.

## Overview of the Internet of Things

IoT is the developing concept where all devices and electronics are connected to the internet to send and receive data, to interact, and to respond to their physical surroundings. The Federal Trade Commission defined the IoT as an "interconnected environment where all manner of objects have a digital presence and the ability to communicate with other objects and people." (FTC, 2015, pg. 1) Much of this concept is already becoming reality.

How does the IoT relate to the everyday person’s personal data? New IoT devices that have begun to be manufactured and marketed as consumer electronics, generate data sets from users and require access to existing personal data. These common household objects are being newly manufactured to include more connectivity features. Conventional smart devices such as phones, TVs, printers, and cameras, were starting points for the IoT. The IoT has now expanded to envelop all the aspects of consumer homes. Automated smart homes include features such as entertainment systems, thermostats, door-locks, lights, ovens, refrigerators, toys and surveillance systems which are controllable through mobile devices. (Shamrihi,1, 2016) Beyond living space, wearable devices make the IoT a part of one’s person like watches, fitness tracking wristbands, and wireless pacemakers or insulin pumps. (Williams, 2016)

While only a few key devices require identifying information to operate, these devices generate enormous amounts of detailed consumer data as they are used. A television could keep track of users’ viewing habits, a room’s lights patterns might indicate when someone is or is not in the room, and a pulse-measuring fitness band can determine the wearer’s general fitness or sleeping patterns.

“Unlike the web domain, which only captures users' online activities, IoT systems can capture users' activities and behaviors 24/7—online and offline—through a variety of devices. Because of this accessibility, however, the IoT domain poses more significant privacy risks.”

- (Perera, Wanjan, Zang, Zamaya, 2016)

IoT devices’ combination of personal data coupled with the cyber security vulnerabilities make them an identity theft target for hackers. (Frustaci, et al, 1, 2017) These vulnerabilities are common due to manufacturer neglect, and development schedules with short time to market, and extensive cost reduction.

## Industry Standards for Consumer Privacy

Data privacy has been an issue studied and addressed by governments since the 1950’s (FTC, 1998, pg. 7) Once the handling of data is taken out of the hands of the individual, consumer protection groups aid in enforcing responsible handling of that data. The Federal Trade Commission released the report, “Personal Privacy in an Information society,” in 1977 to create public policies from and establish some of the first data handling standards. The Fair Information Practice Principles (FIPP) are even more important today considering how often consumers need to access and share data. The following outlines the FIPP which state what a consumer should be informed of before providing personal data to a business.

“- identification of the entity collecting the data;

- identification of the uses to which the data will be put;

- identification of any potential recipients of the data;

-the nature of the data collected and the means by which it is collected if not obvious (passively, by means of electronic monitoring, or actively, by asking the consumer to provide the information);

- whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information; and

- the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data;”

-(FTC, 1998, pg. 7-8)

Consumer Privacy Enforcement by the FTC

Problems arise in the application and enforcement of these principles across different areas of commerce. None of those principles are binding for businesses, and there are no hard and fast general privacy laws in the United States. Instead, we have commissions like the FTC instituted to “investigate, enforce, and litigate claims”. The FTC promotes business self-regulation by relying on customer reports and complaints rather than tedious and costly monitoring of business practices. (Shahmiri, 2016, 31)

When legal action is required, the FTC uses powers authorized by Congress in Section 5 of U.S code, title 15, only if “the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.” (FTC,1994) Section 5 gives the FTC the ability to litigate under two claims, Deceptive Practice, or Unfairness.

Deceptive practice is claimed when a company violates its own privacy policies. An example of breach in contract could include any of the FIPP listed above. A deliberate action example would be a company sharing the collected data of a customer with undisclosed third parties, even though the agreed upon privacy policy stated all information would be kept within the company. A passive or neglectful example would be a company claiming they will use strong data protection methods to prevent easy access to sensitive customer information, while doing none of those things. Whether or not any misfortune happens and damage is done, the claim can still be made, and legal action taken.

Shahmiri lists the conditions in which the FTC can file “unfair practices”,

1. “the practice causes or is likely to cause substantial injury to consumers;
2. (2) substantial injury is not reasonably avoidable by consumers; and
3. (3) the substantial injury is not outweighed by countervailing benefits to consumers or to competition.”

-( 2016, pg. 33)

The security issue is difficult for manufacturers and hardware designers because of the “lack of standards specifically designed for devices with limited resources and heterogeneous technologies.” (Frustaci, et al, 1, 2017). This means that devices with limited computing power and minimal interfaces have less regulation and specifications, leaving room for insecure practices.

## Compromises to Consumer Privacy Standards

This section will cover different case studies where consumers’ privacy was lost. There are many factors and levels at which this can happen, and it is important to understand how any scenario affects the end user. Whether it was a manufacturers’ security defect, a new unforeseen cyber-threat, or a company deliberately infringing on consumer’s privacy, thewill all help to understand the issue more clearly.



TRENDnet Webcams

The FTC summarized its charges against the firm TRENDnet as “lax security practices [leading] to the exposure of the private lives of hundreds of consumers on the internet for public viewing” (FTC, 2014). TRENDnet marketed their cameras as secure and capable of anything from home-security to baby-monitoring. Their fatal flaw was that they “transmitted user login credentials in clear text over the internet, stored login credentials in clear text on users’ mobile devices, and failed to test consumers’ privacy settings to ensure that video feeds marked as “private” were actually private”. (Shahmiri, pg. 33, 2016) Their insufficient data security is a perfect example of deceptive practice.

Mirai

On October 20th 2017 “Hundreds of thousands, maybe millions” of unsecured internet devices were hijacked and used in a massive DDOS attack. The devices were easily controlled once their passwords were automatically guessed using a list of common passwords. A DDOS attack operates by simply overloading a server with data requests from a large number of sources which prevents normal users from getting their data requests filled.

This type of large scale device controlling is called a “botnet”. Botnet illustrates how unsecured devices pose a threat, not only to the device itself but en masse they can bring a large websites’ infrastructure to its knees. Botnets’ existence is not driven by the desire to access a devices’ information, but to use the device itself as a tool against other devices.

Finding a solution to this issue is difficult due to the pervasive neglect by device manufactures to ensure their products are secure. Most security vulnerabilities are unknown until the exploit has happened to other devices and the security fix is implemented via an update from the manufacturer post production. However, many IoT devices are not supported in this manner and are left with factory default security capabilities.

“From a manufacturing and security perspective, the state of IoT devices hasn’t changed, nor did we expect it to. In the short term, IoT devices will continue to be one of the most highly exploitable tools in attackers’ cyber arsenals. We will continue to see massive thingbots being built until IoT manufacturers are forced to secure these devices, recall products, or bow to pressure from buyers who simply refuse to purchase vulnerable devices.”

(Boddy & Shattuck, pg. 5, 2017)

Buyers’ awareness of these vulnerabilities is not yet significantly affecting the market yet. Throughout the next section I will analyze how well informed consumers are about the security of IoT devices.

## Current Consumer Awareness of Security Risks

While some of these security incidents and breaches do reach headlines, research has shown there is still an alarmingly low amount of consumer awareness for IoT devices. Turgut and Boloni in their paper “Value of Information and Cost of Privacy in the Internet of Things” make the comparison of security awareness in the physical world versus the digital world. They propose that it is much easier for us to determine the safety of a public physical space than it is to determine the safety and privacy of a digital site or device. (2017, pg. 62)

Keeper, a leading data security company, performed a survey on current IoT consumers and gave statistics for the largest demographic of consumers

“According to the survey, 65 percent of Millennials said they are not aware of IoT security risks… More than half (53 percent) indicated they plan to purchase IoT toys…Unfortunately, most of these products were created to be first to market and provide convenience to their customers," Guccione (CEO of Keeper password manager) said. "These priorities seem to be top of mind to consumers, too. They want to be the first to have the device and tend to buy them for the convenience factor”

-(Kerner, 2017, pg. 1)

# Proposed Solution

## Description

To best prevent data misuse and increase security, the FTC’s first and “most fundamental” principle of notice should be implemented. (FTC, 1998, pg. 7) The primary aim is to inform and raise awareness of the data being collected from them and the corresponding risks and procedures to be taken to protect their data.

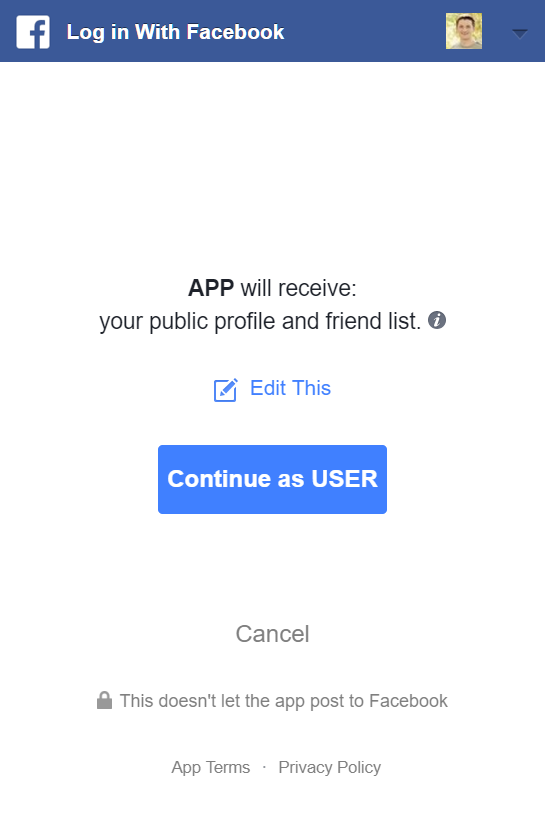


Image 1. Screenshot of Facebook’s permissions page.

Websites and applications have implemented this principle by prompting users with a permissions webpage such as the one presented in image 1. Effectiveness of this method is varied, but its directions and purpose are clear for users. At first glance, it appears to be a P3P approach, where the user either continues or cancels, accepts or rejects the data permissions. But there is room for a more customized user preference using the “Edit This” selection. The strengths of this method are in the required user input, modular privacy settings, and simple familiar terms presented to help the user understand the nature of the data being shared.

IoT devices usually don’t have the luxury of a graphics interface to notify the user of its data policies. Products like the Amazon echo dot, or Samsung Smart devices work by simply plugging in and syncing to a phone.

D. Turgut and his research team in their analysis of IoT security, created a list of requirements for data gathering companies to adhere to. Two of their requirements…

› Data consumers should clearly inform data owners regarding what kind of knowledge is expected to be discovered using their data.

› Data owners should know the risks—their impact level of sharing (trading)—regarding a particular type of data before sharing (trading) occurs.

-(2017, pg. 5)

## Improving Data Security

Detecting security vulnerabilities is a topic in its own right and has a growing pool of research for IoT devices. Many vulnerabilities are detected after the product is released. However, with increased documentation and worldwide exposure to threats, a simulated test environment can be formulated to test for known security threats. Several companies within the past few years have proposed and begun work on an extensive “test bed” for IoT devices.

“The IoT testbed must supports a range of security tests, each targeting a different security aspect. The testbed should detect various vulnerabilities that IoT devices can be prone to and provide analysis and proof of concept to these vulnerabilities.”

(Siboni, Sachidananda, Shabtai, & Elovici, pg. 3, 2016)

## Example Mock-Up

I’ve created an example label to demonstrate the key aspects of informing consumers. Its formatted to work on both box packaging as well as digital displays, so both online and retail customers can be informed about their purchase.

Image 2. Example mockup of a consumer-friendly security mindful label.

This mockup is divided into three sections to help the consumer acquaint themselves with how the device collects and shares data.

Required Permissions

These permissions grant access to the bare minimum data that the device requires to function. This would be the most important part of notifying the customer. With this information a customer should be able to make the assessment if the risk or cost of privacy is worth the benefit the product provides. (Turgut, Boloni, 2017, pg.63)

Secure Device Procedures

These procedures inform the consumer how to keep the data on the device secure from cyber vulnerabilities. Unlike computationally limited IoT devices, complete operating systems can monitor their processes, and detect the need for new software upgrades to provide protection from new security threats.

Opt-In Permissions

These permissions include only optional data-reliant features. Customers should know that these abilities are completely optional before purchase to prevent confusion when setting up the device.

## Anticipated Results

This label can be compared to the Surgeon General’s warning label, but for the field of consumer electronics. Instead of cancer and adverse health effects, the hazards being avoided are identity theft, and invasions of privacy.

Unlike cigarettes’ relationship with Surgeon General warnings, IoT devices can be improved to provide stronger security and better suite customer preferences. As customers are informed about the strength and requirements of the devices they buy, companies will be encouraged to build devices that contain better tested and reliable data security.

## Suggested Further Research

Create Standardized security integrity measure which can be displayed as part of the label. Include notices such as validation for how often and consistently updated the device is and, how well it performed under in-house testing using an aforementioned testbed.

Poll consumer responses and satisfaction with IoT devices with various levels of reputability of security. Determine if userbases are fully aware or informed about current issues. Track down any specific products which cause more trouble than others (currently DVR’s and security cameras)

# Conclusion

Security is guaranteed to remain an issue because of the continual and unprecedented growth of the internet of things. The need has already expressed itself in the disastrous products that have failed to preserve consumer privacy. While most these episodes appear to have been only minorly disruptive, some experts say that this is evidence of just the planning and preparation of larger scale attacks.

Consumers care about how their data is managed. It is within the consumers’ and the business’s best interests to have clarity in data handling intentions and practices. IoT’s new model of consumer products requires a familiar method of informing consumers to help them relate to new concepts. Simple labels spell out the ground level concerns and information consumers need, which can be based off of standardized technical test information.

Security of IoT devices needs to be addressed from many angles. Because of how new the market is, and the highdemand, every aspect stands in need of improvement and standards to be set. Anything from hardware design, software protocols, data encryption and storage, to user implemented security measures need to be driven by a consumer based need. By aiming to inform and educate consumers about the security aspects, they can make better buying decisions and drive the market to produce better suited products.

# References

Amazon. (2017, December 6). Alexa and Alexa Device Terms. Retrieved December 17, 2017, from https://www.amazon.com/gp/help/customer/display.html?nodeId=201566380

Berger, L. (2015, June 23). FTC Approves Final Order Settling Charges Against TRENDnet, Inc. Retrieved December 16, 2017, from <https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc>

Berman, F., & Cerf, V. G. (2017, February). Social and Ethical Behavior in the Internet of Things. *Communications of the ACM,* *60*(2), 6-7. doi:10.1145/3036698

Accession Number: 121046276; Berman, Francine 1,2; Cerf, Vinton G. 3,4; Affiliations: 1 : Edward P. Hamilton Distinguished Professor in Computer Science at Rensselaer Polytechnic Institute, Troy, NY.; 2 : ACM Fellow.; 3 : Vice president and Chief Internet Evangelist at Google.; 4 : Served as ACM president.; Source Info: Feb2017, Vol. 60 Issue 2, p6; Subject Term: Internet of things -- Moral & ethical aspects; Subject Term: Internet of things -- Social aspects; Subject Term: Interpersonal relations; Subject Term: Internet & privacy; Subject Term: Internet -- Safety measures; Subject Term: Decision making; Number of Pages: 2p; Document Type: Article The article discusses the social behavior and moral and ethical aspects of the Internet of Things (IoT), including in regard to privacy rights in the IoT and policy for safety and security concerning the IoT. An overview of the implications of decisions made by autonomous vehicles is provided.

Consumers Want IoT Toys Regardless of Security, Survey Finds. (2017, November 20). *EWeek,* 1-1. Retrieved December 16, 2017, from Computers & Applied Sciences Complete.

Federal Trade Commission. (2015, January 1). *Internet of Things: Privacy & Security in a Connected World* (Rep.). Retrieved December 16, 2017, from Federal Trade Commission website: <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>

Hunt, T. (2017, October 13). Data from connected CloudPets teddy bears leaked and ransomed, exposing kids' voice messages. Retrieved December 16, 2017, from <https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/>

Perera, C., Liu, C., Ranjan, R., Wang, L., & Zomaya, A. Y. (2016, December). Privacy-Knowledge Modeling for the Internet of Things: A Look Back. *Computer (00189162),* *49*(12), 60-68. doi:10.1109/MC.2016.366

Poudel, S. (2016, January 02). Internet of things: Underlying technologies, interoperability, and threats to privacy and security. *Berkeley Technology Law Journal,* *31*, 997-1021. doi:10.15779/Z38PK26

*Privacy Online: Fair Information Practices in the Electronic Marketplace* (Rep.). (2000). Retrieved December 16, 2017, from <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf>

Sanger, D. E., & Perlroth, N. (2016, October 22). A New Era of Internet Attacks Powered by Everyday Devices. Retrieved from <https://www.nytimes.com/2016/10/23/us/politics/a-new-era-of-internet-attacks-powered-by-everyday-devices.html>

Shahmiri, S. (2016). Wearing Your Data on Your Sleeve: Wearables, the FTC, and the Privacy Implications of this New Technology. *Texas Review of Entertainment & Sports Law,* *18*(1), 25-48. Retrieved December 16, 2017, from Academic Search Premier.

Siboni, S., Sachidananda, V., Shabtai, A., & Elovici, Y. (2016). Security Testbed for the Internet of Things. *CoRR,* *Abs/1610.05971*.

Turgut, D., & Boloni, L. (2017, September). Value of Information and Cost of Privacy in the Internet of Things. *IEEE Communications Magazine,* *55*(9), 62-66. doi:10.1109/MCOM.2017.1600625

United States, Federal Bureau of Investigation, Internet Crime Complaint Center. (2017, July 17). *Consumer Notice: Internet-Connected Toys Could Present Privacy and Contact Concerns for Children*. Retrieved December 16, 2017, from https://www.ic3.gov/media/2017/170717.aspx