Recommendation and Evaluation of Liability Litigation Processes for Internet of Things in the Home

Jon Beaulieu, Alex LaGrassa, Alisha Saxena

Department of Electrical Engineering & Computer Science, Massachusetts Institute of Technology

Abstract- The purpose of this document is to brief United States Chief Technical Officer Megan Smith and the Governors' Offices of Technology on recommended changes to product liability law. We suggest reviewing this report and then states enacting laws that reflect the recommendations.

Index Terms- Internet of Things, Consumer Data, Product Liability

Executive Summary

Devices are becoming smarter and more integrated into our everyday lives. The availability of these smart devices coupled with the relative ease of Internet access has enabled the emergence of The Internet of Things (IoT). IoT is a new technology concept that is defined as a system of many interconnected physical devices that process, communicate, and store large amounts of sensitive personal data over an Internet network. An example of an IoT device is a smart thermostat that heats the house based on the user's schedule (Nest). Recently, IoT has become popular in the home, where these devices can automate many tasks based on data collected by their sensors (Paez 31).

However, the always-on, always-connected nature of IoT devices makes them vulnerable to various attacks that can compromise user privacy and safety. Product liability laws are in place to protect consumers by allowing them to sue device sellers, who can then sue device makers as appropriate, for defective products (Steams 5). But these existing product liability laws are not sufficient to protect people who buy IoT devices. These laws do not account for the nature of IoT, because nearly all software introduces security vulnerabilities that can cause major privacy problems. Additionally, the vast quantities of sensitive data collected by these devices are often unprotected (FTC 17). Hence, we propose updated liability litigation processes for Internet of Things devices in the home. Updating product liability laws to reflect the nature of IoT will require two main steps.

First, any sensitive data collected by the devices needs to be protected. To do so, we must refine the definition of sensitive data. Currently, there are legal protections for Personally Identifiable Information (PII), but this only includes a small number of clearly identifiable data points, like Social Security Number (Schwartz 397). We define a new, broader category of protected data: sensitive personal data (SPD). Since aggregated sensor data can reveal sensitive details about a person's lifestyle, emotions, and whereabouts, we set a low threshold for what constitutes sensitive data to err on the side of caution.

Second, we recommend that states update their product liability laws to include software vulnerabilities as design defects rather than givens in software. We identify five requirements that would ensure reasonable device security: 1) data minimization 2) data encryption 3) testing security measures 4) access control and 5) security patches. Software bugs will be considered a design defect if and only if these five requirements are not met

An alternate and potentially complementary approach to improving consumer protection against IoT vulnerabilities is market enforcement: promoting competition in security protection by requiring disclosure of security practices. This allows us to protect consumers by keeping them informed about the security features of IoT devices in a way that may require less regulation and enforcement.

To evaluate these recommendations, we examine some real case studies and compare the possible outcomes of litigation using the existing and proposed IoT liability frameworks.

I. THE INTERNET OF THINGS AND PRODUCT LIABILITY

A. The Importance of Security for IoT

Internet of Things (IoT) is a network of interconnected physical and virtual devices. People use IoT devices for data capture, processing, and communication to provide services. The “thing” in IoT refers to a physical device or virtual object that is integrated into the communication network (ITU 1). IoT is primarily used for convenience or to offer better predictions for future behavior. For example, smart refrigerators can transmit a lists of their contents to users’ smartphones while the users are in a supermarket. Similarly, heaters can be set to turn off as users leave for work, and turn on an hour before they come home, saving energy (Kum 3959).

IoT devices typically serve a different purpose than ordinary personal computers. Personal computers perform tasks and calculations upon request, while IoT devices are ‘always on and always connected’ as they sit silently in the background, collecting and transmitting data to learn more about the user so that they can conveniently assist the user at some future time. This leads to IoT devices exhibiting more vulnerability than typical personal computers exhibit, which can be turned off when not in use.

IoT offers a better experience for users, but this could come at the expense of user privacy and security if a device malfunctions or is not properly secured. To be useful, IoT devices must collect and transmit an unusually high amount of personal consumer data, which raises privacy concerns if the data can be accessed by someone other than the intended user. Data collected from the home could be especially sensitive and private to the device owners. A breach in this data is devastating to consumers, with attackers able to capture every detail of a user’s life. For example, a lot of information about a person’s schedule can be extrapolated from seemingly mundane details about the home. The temperature of the house can indicate when someone is home, or is not, allowing potential home burglars to know when to rob the house. If a user inputs credit card information into a smart television, and the smart television is hacked, the user can potentially lose a lot of money. Smart fitness device hacks can seriously injure a person, like if an internet connected treadmill is suddenly ramped up to 20 mph by a hacker (FTC 12-13).

These risks are very real and must be minimized as IoT devices become more ubiquitous. And yet, annually, IoT devices generate approximately 200 trillion gigabytes worth of this data and store it on various internet-connected mediums (Intel). Thus, reliable forms of security are needed on IoT devices, with regulations and liability laws outlining the procedure for when those standards fail to be met.

B. IoT Security Vulnerabilities

IoT devices are networked, which makes them inherently vulnerable to attacks. Potential device weaknesses that can be exploited include web interface authentication failure, insecure password storage, and unencrypted HTTP requests. Attacking these vulnerabilities can give hackers access to any data on the device or the ability to hijack the controls of the device, compromising the privacy of user data collected by the sensors as well as the physical safety of the user, as previously described.

These vulnerabilities are compounded by the lack of relevant legislation to regulate these devices and protect consumers. For example, when a payment transaction company in Heartland Payment Systems Inc. vs. US, suffered a major data breach, the Texas federal court ruled that it would not be possible to provide absolute security, citing "in today's known world of sophisticated hackers, data theft, software glitches, and computer viruses, a jury could not reasonably find an implied merchant commitment against every intrusion under any circumstances whatsoever.” (Hannaford Bros). It is inevitable that any reasonably complex piece of code will contain some bugs. But if courts generally accept that software cannot be vulnerability-free, it fails to hold software developers accountable for their products.

Our recommendations need to establish a requirement for secure software practice, like access control, encryption, data minimization, and testing. Codifying these requirements would ensure designing for security, and testing against some set of possible attacks. Since the landscape of software capabilities changes, and hackers discover new bugs, the recommended requirements need to include patches when vulnerabilities are found.

II. RELEVANT STAKEHOLDER VALUES

The first step to improving liability law for IoT devices is understanding the needs and values of the stakeholders involved. The large number of stakeholders invested in IoT systems makes the technology a unique and challenging problem to regulate. Many different people are involved in the general process of creating and distributing IoT, including software developers, hardware creators, Internet Service Providers, sellers, and consumers. Each has different values, many in conflict with each other, and it is important to account for these when writing legislation. We have identified three primary stakeholders in the following sections.

A. Developers and Sellers

The employees of the companies or organizations that design and sell IoT devices value their ability to freely develop and sell a product that satisfies customers. Currently, they are protected from litigation for product defects by forcing users to sign service agreements (Bilton). This protection from lawsuits helps save the companies time and money, both of which are valued resources. We must keep in mind that improving the security of a device requires engineering time, because they complicate the design, require extra engineering, and extra testing. All in all, developers will want a policy solution that still allows them the freedom to innovate and make reasonable mistakes without burdensome litigation or a drain on resources. Similarly, sellers want the ability to distribute products to consumers without constant fear of being sued so they can make a profit.

B. Consumers

Consumers buy and use IoT devices, so they would obviously like them to be both functional and secure. Therefore, we need to design our regulations such that they do not overtly inhibit functionality. In other words, we must be careful about limiting data collection, because these devices usually require some sensitive data to perform their intended functions. For example, an IoT device that uses the user's schedule to make decisions about when to turn on appliances must store sensitive data about the user's whereabouts during the day. Hence, these devices inevitably collect personal data that the consumers would like to protect (Paez 37). In addition to being an inadvertent invasion of privacy, these devices, if in the wrong hands, can also be used nefariously to attack the user or his/her home. When proposing policy changes, we must bear in mind that consumer privacy is of utmost importance, as the consumers have the most at stake in the discussed scenarios.

C. State Legislators

State legislators value the opinions of their constituents, in addition to having privacy considerations of their own. They may also consider the value of innovation in their state. By imposing too strict of a liability law for IoT devices, engineers might be disincentivized from either developing or sellers disincentivized from selling their product to consumers in a state who could later sue them. This might stifle innovation. They would also want laws that are relatively easily enforceable, since they will be specifying how to ensure companies and courts follow updated laws.

III. PROTECTING SENSITIVE PERSONAL DATA

Establishing guidelines for protecting sensitive personal data is a necessary step in the process of formulating IoT liability policies. Clearly defining which types of data are sensitive and the manner in which it should be protected will allow us to include specific provisions in our policy recommendations that will aid in determining liability.

A. Problems with Current Data Protection

Currently, some states have created a category of data called Personally Identifiable Information (PII), that is protected by law. If some data is considered PII, that generally implies that it is nonpublic information that can be uniquely linked back to a human. However, there is no uniform definition of the term in US Law (Schwartz 1828). The most common definition for PII is a "specific-types" approach, that enumerates all types of data that are considered PII (Schwartz 1831). For example, under Massachusetts State Law, personal information includes first and last name coupled with Social Security number, driver's license, financial account number, security/access code, personal identification number, or password. Anything publicly available is not considered personal information (Greenberg). Similarly, the FCC defines personal data as first or last name with first initial combined with government issued ID number, banking numbers, access codes, usernames, passwords, or email address (Ruckman 2). While there is no doubt that these specific pieces of information and personally identifiable, these lists are not exhaustive.

When accounting for the fine-grain data collected by IoT devices in large volumes, PII protection laws as they currently stand are not sufficient for IoT users. For example, the temperature of someone's house is not protected under "specific-types" PII definitions, but the time someone is at home can easily be inferred from changes in the temperature of the house. Because IoT devices collect so much intimate information about the home, much about the people who live there, which can be considered personal information, can be inferred. Hence, we must broaden the scope of personal data protection so that IoT users can be adequately protected in case of data breaches.

B. Protecting Sensitive Personal Data

To protect consumers of IoT devices, which collect a large number of datapoints about users, laws that currently protect PII should protect what we define as "sensitive data" too. Protecting personal sensitive data is a broader approach than just protecting PII. This will help ensure that the large amount of data collected remains secure.

All data on an IoT device, especially one in the home, poses a privacy risk. The FTC defines "sensitive personal information" as including "precise geolocation, financial account numbers, health information,...habits, locations, and physical conditions over time"

(FTC 14). Once again, this list is not exhaustive, but is closer to the types of subtly personal data collected by IoT devices. Building on this concept of sensitive data, it is important to protect all data collected by IoT devices because very sensitive and personal details about a person’s life, including mood, stress levels, demographics, happiness, exercise, and schedule can be inferred from rich datasets gathered from IoT. Even something seemingly neutral like radio waves can be used to detect a person’s mood (Stefanovich).

A potential concern is that an attacker can use this information to burglarize a home for instance, because the data reveals a person's schedule. Similarly, sensor data can be used to eavesdrop into a private space. For example, researchers in Germany were able to use unencrypted data from a smart meter device to determine what television show someone was watching. Data from IoT devices can even be used for harassment, discriminatory, or stalking purposes. On a more intimate level, unencrypted camera feeds can be intercepted by hackers into a private space (FTC 17).

Overall, to err on the side of overprotection, we can say that a breach of any of the data on IoT devices could be damaging for the user. The high level of detail in the data makes it necessary to protect all data collected. Therefore, we propose that all data collected by IoT devices be considered personal sensitive data, and fall under the same protections as PII for consumer data protection laws.

IV. LEGISLATION ENSURING PROTECTION FROM DEVICE DEFECTS

The main issue preventing consumers for suing for product liability is the lack of a reasonable standard of care. If there is no standard, then it is impossible to make products that are not up to standard. Once a duty of care is set, then existing liability laws can apply. Consumers can sue device sellers under a variety of legal theories, all of which depend on there being a baseline level of reasonable measures the designer must take to ensure their product is not defective. First, we will look at existing legal theories to show how it falls short for IoT product security. Second, we will demonstrate that current liability for software problems does have laws protecting consumers from obvious misuse or insecure storage of some types of data, although there are limitations to these laws.

A. Existing Liability Law

Because our research is focused on updating current product liability law, we must understand what consumers can currently do to protect themselves using the legal system. Then, we can look at deficiencies or ways that current policy would not work for IoT appliances and make recommendations accordingly.

i. Product Liability Disclaimers

The primary barriers to protecting customers from insecure products are service agreements allowing IoT developers to rid themselves of any blame for product defects. There are no reasonable limits for what customers can agree to in service contracts. For instance, here are the terms of service for Nest, an IoT device company that specializes in devices that monitor the home:

> *“To the maximum extent permitted by applicable law, in addition to the above warranty disclaimers, in no event will (a) Nest be liable for any indirect, consequential, exemplary, special, or incidental damages, including any damages for lost data or lost profits, arising from or relating to the services or the products, even if Nest knew or should have known of the possibility of such damages.*
>
> *Under no circumstances will Nest be liable in any way for any content, including, but not limited to, any errors or omissions in any content, or any loss or damage of any kind incurred in connection with use of or exposure to any content posted, emailed, accessed, transmitted, or otherwise made available via the services.” (Nest)*

Terms of service agreements like the one above are completely legal and protect companies from any blame in case of data breach or other defects of the device. To make it worse, device makers often force users to agree to these terms of service just to get access to the device and its services. In addition to explicit disclaimers stating that customers cannot sue for defects, the complex layers and multiple companies responsible for different parts of an IoT device can effectively shield them from liability by making blame difficult to assign (Noto).

ii. Legal Theories

In this section, we present four existing liability theories that can currently be used as a basis for litigation:

1) Negligence is "failure to exercise that degree of care that an ordinary, reasonable, cautious, prudent person or corporation would have exercised under all the facts and circumstances then existing" (Sweet). Fulfilling a reasonable degree of care requires designing the product safely, inspecting it, testing it, making it from safe

materials, packaging it safely, and providing adequate instructions for use (Steams 5). Consumers can sue product makers for damages due to negligence.

2) Strict product liability can also be a basis for litigation if a product is defective and causes an injury. There are many ways that courts approach strict liability, but generally strict liability implies that the defendant produced defective product in some way, regardless of the defendant's intent. Strict liability puts much more responsibility on manufacturers, requiring them to carry out more rigorous testing to ensure their product is not defective in a wider variety of situations, as the plaintiff does not need to demonstrate that the device designers were at fault or had malicious intent, only that the defect occurred and that it caused damage (Abraham 280).

3) Warranty claims are based in contract law. The Uniform Commercial Code (UCC) governs warranty enforcement. Warranties are a promise about what a product can offer, including what it can be used for and to what extent. Though product liability law is state governed, all states have adopted the UCC (Steams 6).

4) Contributory negligence is a legal theory that accounts for the consumers responsibility if a product does not function as intended. If a consumer sues for product liability, sellers can defend themselves by asserting that the user misused or altered the product (Steams 11). This would also protect manufacturers from sellers altering the product without authorization. For example, the effectiveness of a username and password also depends on the consumer creating a strong enough password.

Although these four theories may be sufficient for pursuing litigation regarding other types of products, this is not the case for IoT devices as the law currently stands. Often, the nature of IoT makes it difficult for courts to protect consumers because the definition of what makes a device insecure is not standardized. As it stands, companies are given the benefit of the doubt when it comes to software bugs, even if it causes damages.

However, we can establish certain guidelines and standards for IoT devices to supplement these theories and provide more protection for consumers. Negligence could protect consumers once there is an established duty of care of IoT device designers. Breach of warranty and contract could apply if IoT terms of service placed some responsibility on the manufacturer rather than the consumer. Nevertheless, victims of product defects may seek damages under negligence, strict tort liability, and breach of warranty, though they are often unsuccessful.

B. Problematic Applications in Case Studies

We will evaluate the effectiveness of the current legal theories described in the section prior by applying them to four real-life case studies representing unique scenarios of compromised security and privacy.

i. Common Software Vulnerability: 2016 DDOS Attacks

In October 2016, a major Distributed Denial of Service (DDoS) attack brought down major websites like GitHub, Reddit, Twitter, and many more. Much of the United States east coast was affected. A DDoS attack essentially floods a website with an unusually high number of requests, overloading the servers and blocking legitimate users' access to the website. This specific attack was carried out by hijacking webcams and DVRs, among other Internet of Things devices for the home, and injecting a publicly available "Mirai malware" script onto these devices (Armerding). In this case, the data integrity was compromised on these devices by exploiting a common software vulnerability.

Under current law, there is no way for customers to sue devicer makers or sellers for negligent design of devices, even if the attack caused damage and there was a known issue. By adding legislation requiring baseline security, US made devices will be more secure because device designers are incentivized to think about security when designing their IoT devices. In addition, since this was a known security weakness, the device makers should have the responsibility to fix the hole via a software update.

ii. Insecure Data Transfer: TRENDnet Baby Monitors

TRENDnet is a network platform that can be used to connect multiple IoT devices so that they can share data and send commands across the network. The network transmits unencrypted login credentials within the network, although at least hashing passwords for authentication is common practice. Through the TRENDnet website, hackers were able to tap more than 700 live feeds from various smart camera devices connected to the TRENDnet network and post them on the internet. The data displayed included babies in people's homes, children playing, and daily interactions: intimate details of a person's life. The authentication protocol used to provide access to the live feeds was deemed insecure, because of the way passwords were handled.

The FTC sued TRENDnet based on its misrepresentation as a “secure” network. This case is under FTC jurisdiction because it is regarding consumer protection against deceptive trade practices (Solove 606).The FTC enforced the need for reasonable security practices to back up claims of “security” by forcing TRENDnet to improve their security practices. (Snell & Lee 4). Although things worked out in favor of consumer protection in this case, a better definition of what constitutes “reasonable security practices” can help simplify these proceedings in future cases.

iii. Device Malfunction: Nest Thermostat

A major issue with IoT devices is service agreements prohibiting customers from suing the company. The terms of service for Nest, cited in section A above, limit damages and require customers to travel to San Francisco for arbitration. Nevertheless, they are still subject to failure, like most home appliances that are subject to basic safety standards.

In 2016, the Nest Learning Thermostat experienced a software bug that caused it to drain the battery and stop working. This left many users in the cold at night. Nest worked on fixing the vulnerability, but this required a tedious nine step fix software update requiring about an hour of the users time, and some hardware shipped out to customers (Bilton). Thankfully Nest responsibly held themselves accountable for the malfunction and took the necessary steps to remedy the issue. However, if users had chosen to pursue litigation and Nest had been slow to respond with fixes, the user would have had very little to no leverage in the courts because the terms of service clearly rids Nest of any blame.

iv. Data Breach: VTech Children’s Toy

Toymakers who sell internet-connected children’s toys are required to ensure that their products comply with the Children's Online Privacy Protection Act, which imposes standards on how much of a child’s data and personal identity can be stored and shared online. The law limits child profile exposure online and gives parents/guardians additional rights to manage their child’s internet presence (Scelsi 72).

In late 2015, VTech, a toy manufacturer that maintains an online app store for their children’s products, experienced a data breach in which an unknown party used a form of SQL injection to access account data for approximately 5 million parents. This information included passwords, home addresses, and IP addresses . Additionally, the attacker was able to access data for the children under each parent’s accounts, which included the name, gender, and age for each child. Although the compromised information was allegedly not widely distributed or sold, the ability to gather such personal information on millions of children and their place of residence presents a host of opportunities for nefarious entities (Kerner).

As the law currently stands, it would be up to the courts to decide if VTech demonstrated negligence in a lack of rigorous testing before releasing the device. Depending on the court, the outcome of litigation could vary.

V. RECOMMENDATIONS FOR NEW LEGISLATION

By examining the case studies, it is evident that there is a need for more specific and clear standards regarding security for IoT devices, and a limitation on the scope of terms of service contracts. We will outline our recommendations in more depth and detail in this section.

A. Product Liability Regulatory Solution

We recommend requiring several security practices for IoT devices in state product liability law. If failure to execute these actions results in damages to customers, they can sue device sellers who can then sue device makers for negligence, strict product liability, or breach of contract where applicable. It is important to draw a distinction between suing device makers and suing device sellers. Device makers are ultimately responsible for designing secure devices and are eventually liable for defects. However, the seller must be sued first as the intermediary in case the products are imported and the foreign manufacturers are not subject to American law. The scope of our recommendations is limited to internet connected physical devices that are available for general purchase.

The definition of a device that needs to adhere to these guidelines is defined in the ITU Overview of the Internet of Things: a device with the ability to communicate, capture, store, and process data (ITU).

Our suggested required security practices for device makers are:

1) Data minimization
2) Data encryption
3) Testing security measures before launch

4) Access control measures to limit unauthorized user access
5) Security patches for known risks

The logistics of the each requirement will be discussed in the following section. State legislators should include each requirement in its product liability law. In addition to these five measures, states also should consider requiring a Common Vulnerability Scoring System (CVSS) threshold. A CVSS numeric score measures the extent to which a networked product is secure against cyber attack. The advantage to using a CVSS score is that it provides a clear measure for how much security is necessary based on various internal and external factors, and has been updated to reflect the latest advances in technology. However, a CVSS audit requires a very extensive and resource-intensive analysis, which some states might choose not to devote the resources to (Touche). In that case, the five prong test detailed in the following section will suffice.

In addition, we propose limiting the scope of terms of service contracts so that companies can no longer include blanket clauses to divest themselves of all liability in case of malfunction. Instead, these contracts must be more specific and reasonable so that the consumer may pursue litigation for legitimate claims.

i. Security Measures to Enforce

The five pronged test was adapted from an FTC workshop on cyber security for IoT devices and the OWASP Secure Coding Practices (OWASP). We also suggest further and periodic review by a committee of cybersecurity experts to ensure an evenly balanced added burden on developers and increased consumer protection. Here, we analyze implementation logistics and interpretation suggestions for each required practice.

1) Data minimization: Data collection should be reduced so that only the types of data that are absolutely necessary for the features of the product to function are collected. For example, if a children's toy for solving arithmetic problems collects constant live camera feed, this is a failure to meet the data minimization requirement, as the camera feed is not needed to solve equations. Data minimization reduces risk by minimizing the amount of data that can possibly be exposed in a security breach.

2) Data encryption: Personal data should be securely encrypted wherever it is sent over a network. The form of encryption is under the discretion of the developer, but should at least ensure that their encryption methods are updated and known to be secure. For example, SHA-256 would be a valid hash, whereas MD5 has been known for years to be easy to subvert. As computers become more powerful, algorithms will phase out, at which point the developer needs to issue a security patch. Encrypting data protects it from man in the middle attacks (when attackers intercept the communications between devices), and provides an extra layer of security. Another possibility is to require encrypted storage on the device, but we do not consider this as necessary as encrypting data being sent over the network, because IoT devices are typically used in the home, so physical access by attackers is unlikely.

3) Testing security: Building appropriate threat models and using penetration testing to determine possible attacks is important to ensure that the system is secure. Black box testing (writing tests based on functionality, not code) is useful for determining what a hacker without access to the internals would find. White box testing (writing tests based on the code written) is a valid way of leveraging knowledge about the system to think about possible attacks. Overall, we recommend using a variety of testing strategies so that device makers account for a variety of risk scenarios when designing a product and have appropriate defenses for these scenarios.

4) Secure access controls: Most cyberattacks and data breaches occur as a result of vulnerable access control systems. For example, the TRENDnet data breach occurred because passwords were sent over the network in plain text, so hackers could login as another user. Determining whether access controls are secure is somewhat subjective, but there are several industry practices that ensure authorized access. Salted passwords protect users from rainbow table attacks (a method used to reverse-engineer hashed string passwords). Only sending the hash of a password also provides a level of protection from man in the middle attacks. Preventing unauthorized access keeps hackers from being able to change or read personal user data.

5) Security patches: Software is powerful because it can be changed after distributing the consumers, yet dangerous because it is hard to ensure a completely bug free product. Requiring security patches when a common security vulnerability is discovered will help keep consumer security one step ahead of hackers, who are constantly finding new ways to gain unauthorized access. Patches are useful when security methods become deprecated. For example, when MD5 was no longer a useful encryption algorithm, it needed to be replaced by a more secure algorithm

(Wang). Vulnerabilities must be patched if they are susceptible to any attack that allows a hacker to cause damage, through either compromising data integrity, or reading user personal sensitive data. If the developers do not issue a patch, the sellers are liable under the prong that they have failed under (such as access control or data encryption). The sellers can then sue the developers. Determining a maximum response time is difficult because fixing a vulnerability can vary widely in difficulty, but a useful baseline is to begin investigation into a solution within one day of bug discovery.

ii. Further Possible Review

The Standards for an Architectural Framework for the Internet of Things, also known as P2413, is an IEEE standards work-in-progress mainly concerned with developing a common architecture to mitigate industry fragmentation. This framework also includes provisions defining what constitutes “trust”, which is relevant for establishing baseline security standards. The outlines of the framework suggest that "protection, security, privacy, and safety' are necessary to establish trust. When P2413 is published, it could serve as further guidance for IoT device requirements (Adams et al.).

iii. Service Agreements and Product Liability Disclaimers

Under our minimal proposed standard for product liability described in section (A) above, companies cannot avoid litigation by putting certain clauses into their service agreements. Similarly, general disclaimers for products in general are disregarded by courts when customers sue for product defects. The same would apply when IoT products fail to meet standards of secure authentication and data encryption. Even if the service agreement states that customers cannot sue the company for defective products, that part of the agreement is void because it violates the law.

iv. Legal Enforcement

Legal enforcement of these measures is necessary to ensure that the recommendations are actually followed. Once states agree on standards that IoT devices must comply with, consumers will be able to sue when there is a defect or insecurity in their devices.

IoT product liability cases can also be civil suits brought to state courts. Hence, we recommend that states update their product liability laws in two ways: update their legislation, and establish precedent with civil cases. Companies creating IoT devices would then be incentivized to follow reasonable security practices because they value their reputation (which would be damaged by lawsuits) and money (which would be lost to legal fees and fines if they face many lawsuits).

Most states will also need to update the “design defect” definition for product defect claims. The revised definition of design defects includes inappropriate data security, such as failing the five requirements. Otherwise, the device itself is defective, not by design.

Jurisprudence constante is the practice of applying legal standards to new cases in a manner similar to how they have been applied in previous cases, usually in the same court. Because revising product liability laws for IoT devices is going to change the way courts would normally rule on cases, it is important that policy changes are reflected in the application of jurisprudence constante. After establishing the extent to which states value secure software, the courts will need to apply the new standards for product liability for IoT devices. This will succeed if (1) IoT devices are correctly identified as IoT and (2) baseline standards are understood and applied (Fon 219). IoT devices and standards are defined in section (A) above.

FTC enforcement under "deceptive practices" is another method of enforcement that can be effective. For example, TRENDnet advertised itself as secure, so the FTC was able to sue for deceptive practices. Under the Commerce Clause, the FTC enforces a common law through lawsuits to protect consumers. However, codifying the law into state legislation provides a more reliable long term solution, especially since the FTC has come under scrutiny for expanded power (Gathani 27).

B. Market Enforcement Alternative Solution

Consumer sentiment is also a powerful way to enforce certain standards in an industry. If consumers are informed about known risks or vulnerabilities in a device, they will likely gravitate towards devices that have lower risks. Consumers value privacy, while IoT device makers value consumer trust. In other words, device-makers have incentive to reduce vulnerabilities in their devices, resulting in consumer incentive to buy these safer devices. As long as a minor amount of legislation is enacted to incentivize device developers, it is in all the stakeholders’ best interests to reduce vulnerabilities in IoT devices. This reduction is driven simply by requiring device makers to inform consumers of the vulnerabilities of each device and letting the free market regulate itself.

Our alternative proposal is to require disclosure of (1) types of data collected and (2) the level of protection the data is given. For example, the customer must be informed on which data is transmitted in plain text versus which data is encrypted, and be given a basic description of how it is encrypted.

i. Regulated Market Model

Informed consumers have been shown to make better decisions when it comes to buying goods or services. Whether for better or worse, consumers will read labels and buy products that align with what they think is good for them. The classic example of this is nutrition facts. When provided nutrition labels, consumers are likelier to choose fat-free potato chips than when they are not provided with nutrition labels (Miller 282).

We can apply a similar model to the IoT industry by requiring the device-makers to inform users of known vulnerabilities and release information about their security practices. This would include informing users which data is stored on the device unencrypted, how their passwords are checked, and what data is collected about them, so customers can make an informed choice on which product to buy. Consumers will make their preferences clear using their wallets and buying power. Because developers value consumer satisfaction, this will urge them to minimize vulnerabilities in their devices.

ii. Industry Self-Regulation

IoT developers and device-makers can also have the option to affiliate themselves with the Better Business Bureau (BBB) to establish a level of consumer trust in their company. This affiliation will allow them to self-regulate, making sure that their goods and services are up to par with the industry standard while earning a letter grade from the BBB for their performance. This helps foster competition between device developers who are trying to improve their ratings in comparison with competitors. The rating would vary based on the industry, but could be based on the OWASP Secure Coding Practices, which checks for specific security practices, like ensuring that password hashing is implemented on a trusted system, or that a number of failed login attempts disable the account (OWASP).

iii. Limitations

This approach requires some consumer education about the security measures taken by device makers and whether those measures are sufficient. If a company encrypts data with MD5, for example, it should also be made clear that MD5 encryption is now considered weak. Hence, consumers need to know which forms of encryption and authentication will protect their data to the level they need. Learning about the different authentication protocols and forms of encryption is nontrivial, but the hope is that the vulnerability levels are clearly communicated using a rating or grading system and that the consumers who care about their data would make the effort to educate themselves about each security feature's limitations. Furthermore, in order to make more informed choices, choices need to exist. There need to be secure alternatives available in the market for security-conscious consumers to use. Otherwise in a monopolized market, this market enforcement approach would not change much.

VI. EVALUATING RECOMMENDED REGULATIONS

To evaluate each part of our proposed regulations and to test the alternative market regulation solution, we will revisit the four case studies originally mentioned in section IV and separately apply both types of proposed regulations. We will then compare the outcomes of our proposed regulations with what would happen under the current legal system.

B. Common Software Vulnerability: 2016 DDOS Attacks

The recent DDOS attacks involved hackers exploiting a known software vulnerability to remotely hijack many IoT devices and overload the servers of many websites including GitHub, Reddit, Twitter, and more. Although this was a known issue, there is no basis for litigation because there was no negligence when the product was being designed--at that time, this was not a known vulnerability of these devices.

i. Proposed Regulations

The proposed regulations would indeed allow the owners of these devices to sue the device sellers and then device makers for negligence, because the device makers have failed our five prong security test under the security patches provision. The attack used was publicly available on hacking forums and is a known form of device-jacking, and there does not appear to have been any concerted effort on the device manufacturer's part to fix this vulnerability (Armerding). In fact, it is not clear whether these devices are even capable of being patched and if the device owners were informed about the newly discovered vulnerability. Under our proposed regulations (Section V), these are all grounds for the device seller being liable for these attacks, because proper measures were not taken to resolve the issue or at least inform the device owners that there is a known issue (Section IV).

There is still a limitation in the extent to which liability for US products would help mitigate the effects of attacks resulting from transnational products. A manufacturer in China is out of US jurisdiction. Manufacturers and developers might move production to a company with less stringent laws to avoid putting in the extra developer time and limit the possibility of being sued. The positive effect would be that US consumers would choose the more secure US products over transnational ones because they are more secure and trustworthy. On a state level, product liability cases are usually litigated in the state of the consumer, but can be litigated in the state where the most products are sold, where the manufacturer is headquartered, and many possible places (Klerman 6). Thus, this regulation would be more effective as more states adopt it.

ii. Market Regulations

Had the device purchasers been aware that the device they were considering for purchase has known vulnerabilities to malware injection, it is highly likely that they would not have purchased the device. This would prevent a widespread attack. However, for vulnerabilities discovered after the device has already been purchased, the regulated market model no longer applies. Instead, industry self-regulation can come into play if the device maker has not taken action on a vulnerability in a timely manner, the consumer can report this to an organization like the Better Business Bureau. This creates an avenue for consumer requests to be heard and resolved by a third party mediator, and can expedite the manufacturers' response to new developments.

B. Insecure Data Transfer: TRENDnet Baby Monitor

Live feeds from over 700 security cameras connected to the TRENDnet network were made public by hackers who were able to exploit the fact that TRENDnet does not encrypt login credentials when transmitting them across the network. In this case, the FTC was successfully able to sue TRENDnet for false advertisement as a "secure" network. Although this specific case fell under the jurisdiction of the FTC because of false claims and deceptive trade practices, had the "secure" network claim not be made, there would not be a solid case for litigation.

i. Proposed Regulations

Under the updated regulations, the main difference would be that even if the company did not claim to be secure, customers would still be able to sue if hackers breached their data. One of the key factors that allowed the FTC to bring the lawsuit was that TRENDnet advertised that they were secure. If TRENDnet did not advertise security, simply being insecure is not a deceptive trade practice, so this case would not be not within the FTC's jurisdiction. In our new system, the consumer would be able to sue regardless because the product is defective due to its lack of secure authentication of private data. Sending passwords in plaintext is clearly not secure authentication, and would be captured by the recommended security testing and data encryption provisions. Reasonable security measures for authentication include hashing, and salting passwords, but neither of these were used.

ii. Market Regulations

In a situation like this, if customers are aware that the baby camera software they are using is insecure and that anyone can access their passwords, it is highly likely that they will change to a new one contingent on there being another option. Having at least one privacy conscious competitor is crucial for market regulation to work when customers use a product they know might compromise their data.

C. Device Malfunction: Nest Thermostat

Nest Thermostat devices malfunctioned and began rapidly draining battery and then shutting off, leaving many people in the cold. Nest immediately began working on a fix, so no litigation was pursued. However, if some users wanted to sue, they would not have much to work with because their signing the terms of service rids Nest of any product liability.

i. Proposed Regulations

Under the proposed regulations, Nest would be held legally accountable for issuing a security patch in a timely manner. Although Nest did take initiative and work to fix the bug, they were under no legal obligation to do so. Customers may also be able to sue for design defects, as we now include software bugs as a defect if and only if it is determined that the five-prong standards were not followed. It would be up to the courts evaluate whether Nest exercised a reasonable standard of care. Nest would no longer be able to write blanket statements divesting themselves of liability in case of product malfunction in their terms of service contracts, opening up an avenue for litigation and improved consumer protection. Considering that after the software bug was discovered, they were working hard on issuing updates, this indicates that Nest is already incentivized to fix problems with their product. There is nothing in our regulations that disincentivizes releasing updates.

ii. Market Regulations

By promoting market regulation, the arbitration confidentiality clause in the Nest Thermostat service agreement would be void. Customers would at least be aware of arbitration for a product defect, and can make more informed decisions about whether to buy the device. Hopefully over time, customers will not buy the device if there are sufficiently many issues to be concerning (Bilton).

D. Data Breach: VTech Children's Toy

The app store of a popular children's toy manufacturer, VTech, was hacked using SQL injection, and many account details, including personal information about parents and their children, were leaked. Under current law, VTech might be sued for negligence, but this would be up to the court's discretion, as there are no specific guidelines for software scenarios like this.

i. Proposed Regulations

Under our proposed recommendations, consumers – in this case parents – would be able to bring a lawsuit against VTech on grounds of security negligence. SQL injection is a well-known and common form of cyberattack against databases, and it would be left to courts to decide if VTech had reasonably prepared their consumer database for such attacks. This lawsuit could be made in addition to the penalty for breaching the Children's Online Privacy Protection Act, which VTech may already incur under current laws and regulations.

ii. Market Regulations

VTech has publicly acknowledged the existence of the data breach and the investigation of the breach by law enforcement, which supports the market regulation ideal against arbitration confidentiality. Additionally, penalties for violations of the Children's Online Privacy Protection Act would be announced publicly, leaving consumers to make decisions regarding purchases of potentially breach-prone products. The publication of such information would hopefully spur VTech and similar companies to incorporate higher security standards into their products and databases.

E. Market Enforcement and Legislative Solution Comparison

The major concern with market enforcement is the often-long adoption time that new technologies and standards have before becoming widespread. It could be argued that in the modern era of computing, where the average user is becoming more privacy conscious, adoption times for security-related features would be much shorter. Additionally, it makes the sweeping assumption that most consumers are concerned about privacy and security. However, because of the aforementioned high sensitivity of the data that IoT devices tend to collect, we recommend that the legal enforcement route is adopted because it will be effective faster and requires less of a shift in the industry and market sentiment.

Evaluating the legislative solution overall, it has performed better than current regulations in each of the four case studies. It leaves room for the courts to interpret the guidelines on a case by case basis, and significantly increases consumers' right to protection. We expect that this solution will succeed in improving data security.

VII. CONCLUSION

Software inevitably contains vulnerabilities. Yet it is needed to collect, process, and store incredibly sensitive data. Consumers value data protection, while IoT developers value developer time and sales. So, our proposed legislation updates will ensure that consumer data is protected even if that requires some more developer time to confirm that the proper security protocols are used. Transparency about how devices process and store data will also help consumers make more informed decisions about how their data is used, and because companies value sales, they will in turn make sure their product is secure enough for customers to want to buy.

In this paper, we propose guidelines to help regulate IoT devices in a manner that makes consumer protection a priority. Currently, highly personal data that is collected by sensors around the home is either unprotected, or protected with inadequate security measures. Our goal is to give consumers the ability to sue IoT device sellers and then developers for design defects stemming from lack of sufficient security. Sufficient security is defined at a high level as providing data encryption when data is sent over a network, and providing secure authentication methods so that authorized users can access the data. Specifications for what constitutes "secure" are defined by a five prong test requiring (1) data minimization (2) data encryption (3) testing security measures (4) access control and (5) security patches. This test, along with proper enforcement, will help further protect the privacy and security of the American people using Internet of Things devices in the home.

References

[1] Abraham, Kenneth S. "Strict Liability in Negligence." DePaul Law Review 61.2 (2012): 271-302.

[2] Adams, Chuck, Gary Stuebing, Ludwig Winkel, and Viacheslav Zolotnikov. "IEEE IoT Webinar: Internet of Things, Architecture and Standards Q&A." Interview by Oleg Logvinov. IEEE Internet of Things. IEEE, 6 Aug. 2015. Web. 29 Oct.. 2016.

[3] Armerding, Taylor. "DDoS Attack on Dyn Could Have Been Prevented." CSO Online. CSO, 03 Nov. 2016. Web. 03 Nov. 2016.

[4] Bilton, Nick. "Nest Thermostat Glitch Leaves Users in the Cold." New York Times. New York Times, 13 Jan. 2016. Web. 1 Nov. 2016.

[5] D. Guinard V. Trifa and E. Wilde. A Resource Oriented Architecture for the Web of Things. In Proc. IoT Tokyo Japan 2010.

[6] FTC. "Internet of Things: Privacy & Security in a Connected World." FTC . FTC, Nov. 2015. Web. 15 Nov. 2016.

[7] Fon, Vincy, and Francesco Parisi. "Judicial Precedents In Civil Law Systems: A Dynamic Analysis." International Review Of Law & Economics 26.(2006): 519-535. ScienceDirect. Web. 4 Nov. 2016.

[8] Gathani, Magdalena. "Internet of Things Report: The FTC Overstepped Its Agency Rulemaking Authority." Business and Public Administration Studies 9.1 (2016): 27-28. Web. 2 Dec. 2016.

[9] Giusto, Daniel, Antonio Iera, Giacomo Morabito, and Luigi Atzori, eds. The Internet of Things. New York: Springer, 2010. Web.

[10] Greenberg, Pam. "Security Breach Notification Laws." NCSL. National Conference of State Legislatures, 4 Jan. 2016. Web. 31 Oct. 2016.

[11] "IEEE IoT Webinar: Internet of Things, Architecture and Standards Q&A." Interview by Oleg Logvinov. IEEE Internet of Things. IEEE, 6 Aug. 2015. Web. 29 Oct. 2016.

[12] In Re: HEARTLAND PAYMENT SYSTEMS, INC. CUSTOMER DATA SECURITY BREACH LITIGATION. 834 F.Supp.2d 566. United States District Court, S.D. Texas, Houston Division. 1 Dec. 2011. Print.

[13] Intel. "A Guide to the Internet of Things." Intel. N.p., 2015. Web. 15 Oct. 2016.

[14] Kaner, Cem, J.D., Ph.D. "Keynote Address." Kaner. Proc. of Seventh International Conference on Software Quality, Montgomery, AL. Kaner, 8 Oct. 1997. Web. 26 Oct. 2016.

[15] Kerner, Sean Michael. "Vtech Admits Lack Of Database Security Opened Door To Hack." Eweek (2015): 1. Applied Science & Technology Source . Web. 8 Dec. 2016.

[16] Klerman, Daniel. "Personal Jurisdiction And Product Liability." Southern California Law Review 85.(2012): 1551. LexisNexis Academic: Law Reviews . Web. 8 Dec. 2016.

[17] Logvinov, Oleg. "P2413 - Standard for an Architectural Framework for the Internet of Things (IoT)." IEEE Standards Association. IEEE, 24 July 2015. Web. 04 Nov. 2016.

[18] Mahony, Ieuan, and Max Bodoin. "Big Data/ Big Target: Are You Ready? Managing This High Risk Security Breach." ACC. Holland and Knight LLP, 4 Feb. 2014. Web. 3 Nov. 2016.

[19] Miller, D L, et al. "Effect Of Fat-Free Potato Chips With And Without Nutrition Labels On Fat And Energy Intakes." The American Journal Of Clinical Nutrition 68.2 (1998): 282-290. MEDLINE Complete . Web. 6 Dec. 2016

[20] Noto La Diega G. & Walden I., "Contracting for the 'Internet of Things': looking into the Nest", in European Journal of Law and Technology, Vol 7, No 2, 2016.

[21] Ohm, Paul. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." UCLA Law Review 57 (2010): 1701-778. Web. 1 Nov. 2016.

[22] OWASP. "OWASP Secure Coding Practices." OWASP . OWASP, Nov. 2010. Web. 6 Dec. 2016.

[23] Paez, Mauricio; La Marca, Mike. "The Internet of Things: Emerging Legal Issues for Businesses." Northern Kentucky Law Review 43.1 (2016): 29-72.

[24] Ruckman, Stephen M.1, and A. J. S.1 Dhaliwal. "The Fcc's Expanding Definition Of Privacy." Journal Of Internet Law 19.4 (2015): 1-10. Applied Science & Technology Source . Web. 15 Nov. 2016.

[25] Scelsi, Chrissie N. "Recent Developments In Online Privacy Laws." Florida Bar Journal 90.1 (2016): 72-74. Academic Search Complete . Web. 8 Dec. 2016.

[26] Schmid, Viola. "Radio Frequency Identification Law Beyond 2007." The Internet of Things 1 (2008): 196-213. Web. 3 Nov. 2016.

[27] Schuermans, Stijn, Michael Vakulenko, and Christina Voskoglou. "Open Source in the Internet of Things." VisionMobile IoT Report Series (2016): 20-22.

[28] Schwartz, Paul M., and Daniel J. Solove. "The PII Problem: Privacy and a New Concept of Personally Identifiable Information." New York University Law Review 86.6 (2011): 1814-894. Web. 3 Nov. 2016.

[29] Seung Woo Kum, Mingoo Kang, and Jong-Il Park. "Iot Delegate: Smart Home Framework For Heterogeneous Iot Service Collaboration." KSII Transactions On Internet & Information Systems 10.8 (2016): 3958-3971. Applied Science & Technology Source . Web. 7 Dec. 2016.

[30] Snell, Jim, and Christian Lee. "The Internet of Things Changes Everything, or Does It? – Your Handy Guide to Legal Issue-Spotting in a World Where Everything Is Connected." The Computer and Internet Lawyer 32.11 (2015): 1-9.

[31] Solove, Daniel J.; Hartzog, Woodrow. "The FTC and the New Common Law of Privacy." Columbia Law Review 114.3 (2014): 583-676.

[32] Steams, Denis W. "Introduction to Product Liability Law." Marler Clark. Marker Clark LLP, 2001. Web. 2 Nov. 2016.

[33] Stefanovic, Stephanie. "Mood-Detecting Sensors Could Improve AI." Process & Control Engineering (PACE) 69.9 (2016): 31. Business Source Complete . Web. 6 Dec. 2016.

[34] Sweet, Jonathan. "MASSACHUSETTS LAW OF NEGLIGENCE." Attorney Sweet. Sweet Law LLC, 24 Apr. 2014. Web. 04 Nov. 2016.

[35] Touche, Deloitte, and CVSS SIG. "Common Vulnerability Scoring System V3.0: Specification Document." CVSS V3.0 Specification Document. FIRST, 26 June 2015. Web. 13 Oct. 2016.

[36] United States of America. Massachusetts Legislature. Office of Consumer Affairs and Business Regulation. “STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH” The Official Website of the Attorney General of Massachusetts. By CMR. Commonwealth of Massachusetts, 12 Feb. 2009. Web. 29 Oct. 2016.

[37] Xiaoyun, Wang, et al. "Cryptanalysis Of The Hash Functions MD4 And RIPEMD." (2005): Inspec . Web. 23 Nov. 2016.

[38] Weber, Rolf H. "Internet of Things – New Security and Privacy Challenges." Computer Law & Security Report 26 (2010): 23-30. Web. 1 Nov. 2016.

[39] Williams, James; Weber-Jahnke, Jens. "Regulation of Patient Management Software." Health Law Journal 18 (2010): 73-112.

[40] Worldwide Internet of Things (IoT) 2013-2020 Forecast: Billions of Things, Trillions of Dollars. Market Analysis 243661, IDC, 2013.

AUTHORS

Jon Beaulieu – S.B. Electrical Engineering & Computer Science, Massachusetts Institute of Technology, jbeaulieu@mit.edu.
Alex LaGrassa – S.B. Computer Science, Massachusetts Institute of Technology, lagrassa@mit.edu.
Alisha Saxena – S.B. Computer Science, Massachusetts Institute of Technology alishais@mit.edu.