Ben Le Cam
Legal Aspects of Business
Professor John Ophaug
May 3rd, 2015

Internet of Things and Legal Considerations

The Internet of Things ("IoT"), which is the connection of objects to the Internet, has been slowly implemented into our lives and is planned to become one of the biggest industries in the world. The internet is already strongly present in our everyday lives and soon we will interact with objects in the same way we do with computers and phones. Data will flow nearly billions of people to a point where there will be billions and billions of data sets about anything, from the time we eat to where we shop to where we entertain.

The devices that will produce this enormous data will be implemented into American households in mass quantities and therefore penetrate the sanctuary of privacy in the country of freedom.

Not only will the Internet of Things change our personal lives, it will affect businesses on massive scales giving live feedback about anything; from the number of people that stand in a specific area of a shop to cleaning robots in a factory that will check on the uptime of machinery.

All this data will be valuable and beneficial to society. However, many risks will arise and the consumers need to be protected against ill-disposed entities that could cause harm physically, financially or even emotionally on a global scale.

The legislation, whether that is in the United States or in the European Union, has yet to fully adapt to Internet. It is still transforming itself to adjust to the massive cultural shift that Internet brought into our modern societies.

The Internet of Things will make our lives better, but there are a lot of security and privacy aspects to consider. Objects will be able to share a vast amount of data with corporations and governments, yet there is not an easy and legal way to protect against the danger that it represents. There remains to be established a common ground for everyone to understand the legal aspects of smart, connected devices.

In this paper, I plan to develop on a couple Internet of Things devices in order to give a better understanding of the subject. I will then briefly discuss the risks associated with data arising from many sources and shared to corporations about our daily lives. From there, I will take a look at the current legal frameworks that apply to the Internet of Things: whether that is from a Children protection standpoint or a consumer privacy point of view. Additionally, I will briefly mention a case in which the Internet of Things revealed itself to be useful in a positive way to the Court. Finally, I will discuss a personal idea that could be used to better regulate and frame the Internet of Things through the creation of a new set of laws and an institution that would act as a guardian of the US consumer privacy.

The Internet of Things represents the objects that are smart and connected to a network. *Smart* implies that the object is able to make decision on its own without any human command. For example, smart blinds would close whenever the luminosity outside falls beyond a certain threshold. Saying that an object is connected to a network means that it is communicating with other devices such as computers, smartphones or other objects. The connectivity can be local- for example in a house, blinds can communicate with the thermostat, or globally- security cameras can be watched anywhere in the world as they stream their data to servers, which I can then use a computer to connect to the servers.

One of the most well known smart devices is the Nest Smart Thermostat. It is a thermostat that regulates the house temperature based on multiple variables such as current temperature, outside temperature, humidity, personal preferences, expected weather among other data. Nest was developed in 2010 in Palo Alto, California and has been shipping millions of its products. Google recently acquired Nest for 3.2 billion dollars.

Amazon, the online giant marketplace, recently released its Dash button. The Dash button is a simple physical button that purchases the associated product with a one-click touch. For example, you can have a Tide-laundry detergent button that will order a pre-determined quantity of detergent when the button is pressed. It is a genius move for merchants, yet an ethically and legally questionable practice.

The next two devices that I want to introduce are somewhat similar in the legal issues they raise. The first one is the Narrative Clip camera. It is a small clip-on camera that automatically takes a picture every thirty seconds. It is extremely discreet and will let you to look at all the photos via a smartphone or computer. The second one is the Google Glasses. It is a pair of glasses that embed a camera and a microprocessor along with an optic lens on which is projected information. Only you can see the screen, where it is possible to take pictures as well as record videos without anyone noticing.

Sensors will be everywhere, at the risk that owners of such sensors can collect any data about anyone that passes around. For example, the marketing firm Renew developed trashcans that integrated Wi-Fi chips that were capturing the unique identifier of smartphones in order to see how many people were seeing the advertising board. This made a lot of sense from an advertising standpoint however users were not so happy about it since these unique identifiers give the company the possibility to identify recurring

people, to see where they have been, where they are heading and most importantly is not an action for which the users was given the possibility to choose.

The Internet of Things is an extremely exciting field that will certainly benefit society. However, there are risks associated with such a transformative technology. In its January 2015 report "Privacy and Security in a Connected World," the Federal Trade Commission identified three major risks associated with the Internet of Things. These three risks were reported by a panel of participants in a workshop organized by the Federal Trade Commission.

The first risk, unauthorized access and misuse of personal information, is the theft of consumer's data from a corporation. This risk is not specific to the Internet of Things, as we have seen recently with the major attack against Target that resulted in millions of credit card information being stolen.

The second risk is the facilitation of attacks on other systems on the network, which is the possibility of attacking more sensitive systems using a breach of security in a device. For example, one could lock owners in their own house by forcing the lock of the blinds through forcing the light sensor to send low luminosity values.

The third and final one is the risks to personal safety. It relates directly to the previous example, but could be taken a step further if a smart automated system is given more power as for example the management of water filtering.

The Federal Trade Commission also noted that the participants of the workshop discussed the important topics about the Internet of Things. The first one was security; participants believed that security should be integrated as part of the design process of the devices instead of after the product is shipped. Second, the participants stated that

companies should limit the amount of data they collect and dispose of. Lastly, the Federal Trade Commission discussed the notion of choice, which was already brought up earlier.

There are few legal frameworks that apply directly to the Internet of Things, however, it is possible to use indirect frameworks to prevent abuse.

The first one is privacy, which is a human right. However, the definition and what privacy entails is rather vague, especially in the United States. According to Jennifer Winter in her paper "PRIVACY AND THE EMERGING INTERNET OF THINGS: USING THE FRAMEWORK OF CONTEXTUAL INTEGRITY TO INFORM POLICY," there are no comprehensive laws to protect consumer privacy. She first mentions the Electronic Communications Privacy Act of 1986 at the federal level.

She then proceeds to explain that United States citizens must rely on the self-containment of corporations because the Electronic Act does not specifically protect data aggregation and any other novel practices.

Some corporations actually made this aggregated data part of their business model; the best example is Nest Labs. Selling devices is, in reality, not the most profitable activity for Nest. Nest sells aggregated data to energy providers around the country and soon internationally about energy demand. The goal for energy providers is to better regulate the supply since the most expensive part of furnishing energy is to store energy in excess. This is amazing from an environmental standpoint: through better management of energy demand, provider can adjust their production and thus only produce what is necessary. However, energy providers could soon be given the possibility to control your energy-use by turning down the heat or air conditioning systems without telling you in order to optimize their infrastructure. This is something that has not happened yet but energy

providers are huge proponents for that feature as they currently pay $40 per user per year to receive aggregated data. This is over 128 million dollars in revenue for Nest… How can the consumer be certain that Nest won't sell more than just aggregated data?

The concern reached a new high since Google acquired Nest for $3.2 billion, raising awareness about the danger of Google now owning Nest data and making use of it globally. Critics have been speaking-out and thus Google promised not to integrate Nest's data into its infrastructure.

Privacy is again a major concern. Assuming that energy providers can now control our energy use, what else will we be willing to give up for better comfort? With its new physical button, Amazon just reached a new stage in households. It gives Amazon the possibility to understand better who make the decision about households, when the decisions are made, etc.

A great illustration of the risks of connected devices is the Robbins v. Lower Merion School District case. From 2009 to 2010, two high schools in Philadelphia reportedly spied on students in their homes using the webcams on the laptops that were provided by the school. The school also kept a log of websites visited and took screenshots of their screens. Some of the pictures taken by school officials included students sleeping, partly undressed, family members and friends shot on their behalf and other extremely illegal actions. The case raised the question of privacy of students and the right of institutions to spy. But the real concerns were that there was not any legislation against illegal cyber voyeurism. Thus, was introduced a law that clarified that it is illegal to capture silent visual images inside a person's home.

On February 23, 2010, U.S. District Court Judge Jan DuBois granted victim's request ordering the school district to stop remotely activating cameras and taking screenshots. It was later ordered that the school district must pay the legal fees incurred by the victims.

The Electronic Communications Privacy Act, and more specifically Title II: Stored Communications Act, addresses voluntary and compelled disclosure information held by third-party Internet service providers. It states that data owned by the said third-party should not be divulged to other parties, including other customers, partners and providers. However, it allows to divulge information if consent is given. Unfortunately, Title II does not mention anything about a time limit concerning data retention, neither does it limit the capability in which a service provider can collect data, and nor does it restrict the kind of data that can be collected.

This data could be protected by the Fourth Amendment of the American Constitution: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." However, the Fourth Amendment does not specifically state anything about privacy concerning online behaviors and it is therefore hard to apply it in the modern, connected setting.

Under Section 5 of the Federal Trade Commission Act, the consumer appears to be protected against deceptive and unfair practices: "Unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce are hereby declared unlawful." A practice is judged deceptive if it is likely to misled the consumers and if it could play an important role in their decision. A personal anecdote to illustrate this concept is my trip to

New York City two years ago, for which we booked a hotel that advertised a rooftop with view on the Empire State Building. Once there, we realized quickly that the rooftop was closed for work. We had booked this hotel because of the roof top that was advised on their website, thus we were misled in our decision-making process by the hotel's advertisement.

On the other hand, an unfair practice is likely to harm the consumer either physically or economically, that is not reasonably avoidable by consumers and that it is not outweighed by the benefits to the consumer or competition. For example, if Nest would force the blinds to close to save energy with no way for the consumer to stop it, it would be an unfair practice towards the customer.

Another aspect to be considered when it comes to the Internet of Things is the protection of children. The Children's Online Privacy Act ("COPPA") prohibits the collection, use or disclosure of personal information from children under the age of 13 without appropriate parental notice, choice and consent. It was updated on July 1st of 2013. For example, the Narrative Clip camera, a device clipped to your shirt and that will take pictures every 30 seconds, is used to record your day so that you can visually have a memory of every aspect of your life. However, there are many legal issues that can be raised with that technology. For example, what happens to the pictures in which we can see minors? What about people who do not want to be photographed, especially in their own homes?

Consumer's health is a very sought market in the Internet of Things industry. One of the most successful products in this industry is the Vitality GlowCap, a device that knows when you need to take your pills and reminds you if you forgot. There are currently two acts that protect consumers against malicious entities. The first one is the Health Insurance Portability and Accountability Act that was voted in 1996 by the congress. It aims to reduce

healthcare fraud and abuse, to define standards across the industry about the retention of healthcare information and to require the protection and confidential handling of protected health information. Furthermore, the HIPAA Privacy regulations also require businesses to store only the minimum necessary information needed to conduct business properly. This guarantees that health-related data of consumers are limited and guarded safely by health providers and their third-party partners.

Another act that could be used to protect consumers is the Fair Credit Reporting Act ("FCRA") that protects consumers against discrimination through the determinations of credit, insurance or employment. This would protect consumers against the use of personal data collected through applications and devices that deal with purchases. For example, the Amazon Dash Button would give the possibility for cyber intruders to recover someone's spending habits, and thus to estimate their financial situations. Collaring this data with geo-location could give more than any information about the consumer to give intruders the potential to blackmail. Without even going that far, it would be possible for advertising agencies to advertise anyone based on their financial situations. For example, if a consumer purchases a lot through Amazon, yet makes frequent trips to a financial credit corporation, the consumer could be identified as a person that has poor financial literacy and thus be taken advantage of over the internet with targeted advertising. Such practices do exist already on the internet, but the Internet of Things could take it to a whole other level.

While smart devices can bring potential risks and harms to consumers, it can also be used as evidence and even witness in Court. In November 2014, the Canadian law firm McLeod Law, based in Calgary, used data from a FitBit wearable device to prove that the plaintiff never restored her full active lifestyle. The young woman was a personal trainer

when she was victim of personal injury. Since then, she has never been able to recover her full physical abilities. The FitBit is a smart bracelet that tracks physical activity and upload them to Internet giving the users the possibility to review how much energy they burn. The plaintiff was not using any devices before the accident happened, about four years ago, but by comparing her energy levels with other women of the same age and similar physical attributes using an online database, her lawyers hoped to be able to prove that the accident has transformed her and that she was unable to continue her professional activity. This case suggests that not only will the Internet of Things challenge the limits of law about data privacy and security, it will also challenge the way Justice Courts make decisions.

According to the FBI, a digital evidence is an "information of probative value stored or transmitted in digital form. In the FitBit case, we thus consider the data produced by the device as a digital evidence. However, it is legitimate to wonder if that makes the FitBit a witness. The legislation is not really precise about defining the nature of a witness. Will objects be considered as valid witnesses? Will there be a difference between object witnesses in public space versus private space?

For example, if the Narrative Camera takes photos of a crime happening in the streets, is it legitimate material for a judge? What about if this picture is taken in the personal sphere without the approval of the owner? There will need to be more cases similar to the FitBit one in order to detect an emerging pattern.

The Google Glasses, glasses that integrate a camera and a lens to give the consumer useful information is a perfect example of this paraxial situation. There have been many cases of people asking Google Glasses' owners to take them off as they saw it as a threat to their personal privacy.

Before I proceed to explain my personal solution to protect the American consumer, I want to mention the Federal Trade Commission. The Federal Trade Commission is an independent agency of the United State government that promotes fair business practices and consumer protection. In its 2010 report "Protecting Consumer Privacy in an Era of Rapid Change," the Federal Trade Commission advised to take steps toward three specific directions in order to prevent the risks of the Internet of Things.

The first advice is to design devices with privacy in mind. This means that the technical architecture behind the objects and systems need to be conceived with the idea of keeping data private. This includes protecting data against external threat, to limit the collection of data, to be reasonable about the duration of retention of the data and to be accurate about which data is being collected. This relates a lot to the HIPAA.

The second one is to offer consumers the choice, meaning that consumers should have the choice concerning the collection and use of their data every time data is being collected or used. The possibility of having a "Never share data" option should be mandatory for most data collection request. This obviously excludes the context of order fulfillment, internal operations, fraud prevention, legal compliance, first-party marketing and contextual advertising.

Transparency is the third point evoked by the Federal Trade Commission. There should be a way to clearly see what data is being stored, for how long and how it is being used. This should be accessible from a consumer's perspective. Plus, companies should request consumer's permission to use data in any other way than originally agreed. Furthermore, there should be greater education delivered to consumers about their rights when it comes to private entities and data.

In January 2015, the Federal Trade Commission (FTC) issued a report on the Internet of Things called "Privacy and Security in a Connected World." In this report, based on a workshop with experts in different industries, the Federal Trade Commission identified major risks with the Internet of Things that could harm consumers: unauthorized access and misuse of personal information, facilitating attacks on other systems on the network and creating risks to personal safety. The Federal Trade Commission also note that the participants of the workshop discussed the important topics about the Internet of Things. The first one was security, participants believed that security should be integrated as part of the design process of the devices instead of after the product is shipped. Second, the participants stated that companies should limit the amount of data they collect and dispose, of the data they don't need anymore. Lastly, the Federal Trade Commission discusses the notion of choice already brought up earlier.

When it comes to legislation, the participants of the workshop seemed more dispersed. Most participants support the need of legislation, however they also state that a set of laws would be too early to implement as there is still a lot of innovation to be done in the industry. All of the participants however recognized that the legislation would need to be "strong, flexible and technologically neutral."

From a personal standpoint, I believe that the Federal Trade Commission is looking in the right direction. I firmly believe that it would be necessary to have an independent institution that regulates the Internet of Things such as what the Internet Corporation for Assigned Names and Numbers, commonly known as "ICANN," does for the Internet. ICANN is responsible for managing and maintaining the Internet. Even though the Internet was designed to be independent, I think that the Internet of Things will require a process for

business and institutions to be able to collect data. In my opinion, there must be a two-step process. First, a business or institution would need to get permission from the said-organization to require data. This process would involve describing the type of data being collected, the frequency at which it is being collected, the duration of the retention, who will be given access to this data and lastly the process through which the user is being given the opportunity to choose to share its data. Furthermore, it would ask the entity how the data is being stored, and what the measures of security are. It would be required for a safe environment in the future that such an institution gets created to require corporations. For example, back to Nest, they would be required to share that they collect the temperature of the house every thirty seconds, that they collect the humidity level every minute, and also that they collect presence activity about each family member. Temperature and humidity being pretty random variables, the organization would allow such practices but would warn Nest about the collection of data concerning presence. It would also ask Nest how long they plan to keep this data in their system for, and cap its data retention to a certain duration. It would also require Nest to share how they plan to ask the user's permission in a non-obscure way. The organization would here be trying to avoid obscure "Terms and conditions" and force businesses and institutions to be transparent.

When it comes to security, businesses and organizations would have to comply to security measures such as the ones provided by the Department of Defense in its cyber strategy white paper. For example, a procedure such as emergency deleting data in case of intrusion should be possible both remotely and locally. Plus, the storage of data concerning citizens should be domestic.

The organization would stand at the federal level in order to avoid loopholes for corporations operating in multiple states and avoiding a pro-corporation judgment. The organization would need to be publicly funded in order to avoid influential moves from corporations. It would also require its members to be elected through a democratic process. An interdisciplinary team of experts in multiple fields would lead it: legislators, computer scientists, data scientists, politicians etc.

An issue with such an organization would be that these pro-American conditions would raise issues outside of the United States. Thus, a global institution that would define standards policies and best practices around the world would also be beneficial for the development of the Internet of Things.

Such a global institution would define standards in communication, data retention, data structures and more. It would be required for a business or institution seeking to do business outside its country of incorporation to comply with such rules. Thus, citizens of other countries would be insured that the said-entity complied with standards that protect them against fraud, abuse, etc.

For the development of such a global institution, funding would be needed. It would certainly fall under the responsibility of the Organization for Economic Co-operation and Development to fund such an institution.

Perhaps, the best solution would be the development of a label, just like the Green Energy Label. A label would be given to companies and institutions that complied with standards and practices. Such label would be specific to each country, and would require entities to share all the information concerning the data, just as described in the domestic organization section. There could certainly be multiple levels of labeling. First level

("bronze") would insure the users that the type of data being collected is verified by an institution. Second level ("silver") would insure the first level plus that the data is being retained for a fixed amount of time. Third level ("gold") would insure the first two levels plus that the data is accessible to consumers and that it is easily to request its deletion. Fourth and last level ("platinum") would insure consumers about all three levels plus that the data is being stored and guarded according to the highest standards of security in the industry.

The Internet of Things is a very vague yet extremely powerful concept. It is an early stage market and industry that is growing exponentially. So too are the risks, problems and legal concerns associated with it. We have seen in this paper that the risks related to the Internet of Things are somewhat different than the ones associated with Internet. There are common risks, but the Internet of Things will bring a more physical presence that could cause bigger damages to the population.

There are a few existing frameworks that exist already, some of which are being updated to satisfy the risks of Internet. The HIPAA guarantees people that their health data will remain private, the Children Prevention act ensure parents that their kids won't end up on Internet, the Electronics Act somewhat protects consumer's privacy. Yet, there is a need for a new framework to be developed to respond to the future, a future that we can't yet determine exactly.

The current legal system is definitely not ready for what is coming, and just as we are still learning from the Internet and its consequences on society and law, it will take multiple years to respond to the changes incurred through the Internet of Things.