Privacy and IoT’s Battle Royale

Airi Chow (#40003396)

Concordia University

Department of Computer Science and Engineering

Undergraduate Program Director: Dr. Shiri Varnaamkhaasti

Fall 2020

December 12th 2020

‘I certify that this submission is my original work and meets the Faculty's Expectations of Originality’ – Airi

Faculty of Engineering and Computer Science
Expectations of Originality

This form sets out the requirements for originality for work submitted by students in the Faculty of Engineering and Computer Science. Submissions such as assignments, lab reports, project reports, computer programs and take-home exams must conform to the requirements stated on this form and to the Academic Code of Conduct. The course outline may stipulate additional requirements for the course.

1. Your submissions must be your own original work. Group submissions must be the original work of the students in the group.
2. Direct quotations must not exceed 5% of the content of a report, must be enclosed in quotation marks, and must be attributed to the source by a numerical reference citation[1]. Note that engineering reports rarely contain direct quotations.
3. Material paraphrased or taken from a source must be attributed to the source by a numerical reference citation.
4. Text that is inserted from a web site must be enclosed in quotation marks and attributed to the web site by numerical reference citation.
5. Drawings, diagrams, photos, maps or other visual material taken from a source must be attributed to that source by a numerical reference citation.
6. No part of any assignment, lab report or project report submitted for this course can be submitted for any other course.
7. In preparing your submissions, the work of other past or present students cannot be consulted, used, copied, paraphrased or relied upon in any manner whatsoever.
8. Your submissions must consist entirely of your own or your group's ideas, observations, calculations, information and conclusions, except for statements attributed to sources by numerical citation.
9. Your submissions cannot be edited or revised by any other student.
10. For lab reports, the data must be obtained from your own or your lab group's experimental work.
11. For software, the code must be composed by you or by the group submitting the work, except for code that is attributed to its sources by numerical reference.

You must write one of the following statements on each piece of work that you submit:
For individual work: **"I certify that this submission is my original work and meets the Faculty's Expectations of Originality"**, with your signature, I.D. #, and the date.
For group work: **"We certify that this submission is the original work of members of the group and meets the Faculty's Expectations of Originality",** with the signatures and I.D. #s of all the team members and the date.

A signed copy of this form must be submitted to the instructor at the beginning of the semester in each course.

I certify that I have read the requirements set out on this form, and that I am aware of these requirements. I certify that all the work I will submit for this course will comply with these requirements and with additional requirements stated in the course outline.

Course Number: **ENGR 411** Instructor: **Dr.Shiri Varnaamkhaasti**
Name: **Airi Chow** I.D. # **40003396**
Signature: **AC** Date: **December 11th 2020**

[1] Rules for reference citation can be found in "Form and Style" by Patrich MacDonagh and Jack Bordan, fourth edition, May, 2000, available at http://www.encs.concordia.ca/scs/Forms/Form&Style.pdf.
Approved by the ENCS Faculty Council February 10, 2012

Introduction

Technology now makes up a significant part of our lives. Over the last few decades, the increasing availabilities of technological devices and the creation of the Internet has led to a technological revolution highly unthought of by our ancestors back in the 1900s. But with any revolution, this comes at a cost. Internet of Things or better known as IoT consists of devices that can connect to the Internet. IoT had just been computers, laptops or smartphones but over the recent years, the range of devices spanned across different domains from smart light bulbs to refrigerators to other analogue devices that never needed connection to the Internet to function. For the scope of this paper, we will be focusing on IoT related to 'Smart Home technologies' which consist of smart devices used by consumers in their home environment. This paper will give a brief overview of IoT and Smart Homes, explain the current issues relating to privacy, security and ownership and the potential ways to mitigate each of these issues.

IoT and Smart Homes

Before diving into the issues related to IoT and in particular smart home technologies, we need to clarify what exactly are these technologies. Based on the Internet of Things' Wikipedia, it mentions that IoT technologies tend to be related to 'smart home' or home automation (Wikipedia Contributors, 2019e). Automation is associated with the term 'automatic' which based on the Oxford English Dictionary is defined as "working by itself with little or no direct human control" ("Automatic," 2010). IoT technologies can include the most mundane of devices such as lighting, cameras, digital book readers, TVs, watches, blinds, speakers… Most of the time, these devices are controlled with a controller like a smartphone, but now voices and hand gestures have become other options of control. A common trait is their tendency to allow connection to the Internet and potentially communicate with other IoT devices within the same environment.

Regarding a similar environment, Smart Home technologies are a subset of IoT but with a focus on the home environment. Taking a glance at any online shopping catalogue, one can find numerous ways to transform their home into a 'Smart Home'. Some of the common IoT in addition to laptops, desktops and smartphones are security cameras, TV, speakers, lighting and heating. Many previously analogue appliances such as refrigerators, dryers, laundry machines and ranges are now claimed as IoT as many of them allow remote connections via a smartphone app.

Although these IoT have brought along benefits such as convenience, personalisation and accessibility, we must be aware of the risks that we are trading off for these benefits. In addition to concerns related to privacy, there are concerns in areas like security and ownership which are all common concerns when considering any digital goods versus any previously analogue-only goods. Thus, we will first explore these current issues then talk about the potential ways to mitigate these problems found about in most present-day IoT.

Current Issues associated with Privacy, Security and Ownership

Privacy in this paper defines that each individual has an anonymous identity. We should not be able to distinguish or characterise an individual with the data that they provide. Security on the other hand defines that individuals are free from threats. So, an individual's security is threatened if they have to modify their behaviours because of an external factor (e.g. fear of their data getting leaked because of a software bug). Finally, Wikipedia's definition of ownership defines it as "the state or fact of exclusive rights and control over property […]" (Wikipedia Contributors, 2020a). Hence, ownership is the limitation of what an owner can do with their property. Privacy, security and ownership are distinct categories but with IoT, these three categories are commonly found together.

The first issue is privacy but in particular, it's about the excessive data collection and the lack of anonymity. When discussing IoT, the consumers and researchers' main concerns tends to be about data privacy. In the journal article, *"The Internet of Things: When Things Talk Among*

Themselves", one of Ohlhausen's concerning question was "How to achieve the benefits of the Internet of Things while reducing risks to consumer's privacy" (Ohlhausen, 2013). IoT themselves do not lead to issues about data privacy rather it's how the companies implement their data collection. The companies do need the consumer's data to personalise their products, but some companies do not respect the 'Privacy Act' (Canada, 2018) and collect much more data than necessary. Concerning 'Big Data', Wikipedia mentions that "By 2025, IDC predicts there will be 163 zettabytes of data" (Wikipedia Contributors, 2019d). But the main issue is assuring that the law enforcement fine these companies heavily for violating the law of selling the consumers' data to 3rd party without their full consent (which we'll come back to shortly in the ownership issues section) or for just collecting more data than necessary. It shouldn't be the consumer's responsibility to read through the lengthy and legal jargon-filled 'Privacy Act' (Government of Canada, 2019) to assure themselves that the product that they will purchase for their home uses their data appropriately which leads us to another issue about data privacy, anonymity.

Having a smart home shouldn't be the equivalent of letting someone come to your home as they please and cultivate whatever data they like about you. Anonymity helps ensure that the data from your smart home is kept private from only the party's that require this data and to not be able to directly identify you as an individual. But with IoT, it's difficult to know how your data is kept by the company. What got strip away from your data when it gets sent from your Alexa device? (Wikipedia Contributors, 2019c) Are the companies doing enough randomisation and cleaning of data that they keep what they need and discard the rest? These are just some questions revolving around anonymity. The problem with collecting a lot of extra data is that the companies are now responsible to keep this information secure from the external party which leads us to IoT's security issues.

Alongside privacy issues, security issues are also found in IoT. The two main concerning security issues are keeping the data secure from 3rd parties and ensuring security despite the IoT's hardware limitations. With the immense amount of data collected from IoT, consumers place more trust in the known brands and manufacturer that their data is protected from cyberattacks (Zheng et al., 2018). However, there have been studies done such as in the journal *"Network-Level Security and Privacy Control for Smart-Home IoT Devices"* that shows that this protection is lacking. Some of the most common IoT's security concerns are being able to intercept the data sent, sending a denial of service attack on the devices and unauthorised remote access to the device…

Manufacturers may argue that since consumers want lower-cost goods, they need to cut corners because the IoT devices have limited hardware capability but they are still responsible for protecting the consumers against these attacks. It shouldn't be the consumers' who might not have a technical background responsibility to set up the devices in a secure way. Nor should the consumers have to adjust their way of living drastically so they aren't 'hacked' in their own home by their IoT. For example, the default configuration setting on the devices shouldn't use default passwords as stated in *"The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved"* that "In 2014, WeLiveSecurity team highlighted the discovery of 73,000 security cameras with default passwords" (Zhou et al., 2019). Or claim that the devices are secured despite not being so as in the SecurView camera case where "the company claimed that the cameras were secure, they had faulty software that allowed unfettered online viewing by anyone with a camera's Internet address" (Ohlhausen, 2013). So what exactly should the consumers be responsible for when they purchase a new IoT for their home then? This leads us to issues related to ownership.

Ownership is a tricky issue when it comes to IoT. IoT's ownership issue is similar to that of digital goods versus physical goods. The frequently asked question is what exactly do you own when you press the 'buy now' button for a digital good versus a physical good purchase? This is an interesting question to consider because it entwines two particular rights, 'personal property rights' and 'Intellectual Property(IP) rights'.

When you legally purchase a physical good, you can do as you please with it regardless of how displeased the IP holders are. For example, you sell your game in a used game market, give it to a friend or ship it across the globe to another client to use in their region. When it comes to digital goods, it's very difficult to do the same thing because of the digital management systems, prevention of reselling, creating additional copies… So although you might see the 'buy now' button on Amazon for two similar titled goods, one being physical and the other being digital, they are not the same. The former gives you rights as an actual owner whereas the latter tends to provide conditional permission usage rather than digital ownership.

IoT is made up of both types of ownership: physical which is the hardware component such as the device and digital which is mainly about the consumer's data and the IoT's software. The issue is being able to distinguish who's the true 'owner' of the IoT and provide them with the clear rights of their limitations. What do these IoT consumers own? What about their data can they withheld? What can manufacturer as IP holders of the IoT prevent their consumers from doing legally and what are just preferred restrictions that they want to impose? All of these are just some questions related to the issues of IoT's ownership for both the consumer and the manufacturer. Similarly to the issues above, ownership alongside privacy and security are all categories that should be addressed with the creation of each IoT. In the next section, we will explore various potential ways to mitigate the issues associated with these categories.

Possible Mitigations for Privacy, Security and Ownership Issues

Although there are numerous concerns to resolve, we will discuss possible mitigations for the following issues: for privacy, the key issues are regarding the excessive data collection and anonymity; for security, the key issues are regarding securing data from 3rd party and working with the limitation of IoT hardware to provide security and finally for ownership, the key issues are regarding providing a clearer distinction between physical and digital ownership and more insights in what the IP holders/manufacturer's legal rights are versus the consumer's legal rights are regarding IoT.

Starting with privacy, the FTC discusses that the government officials and law enforcers should be kept updated with the latest technological news to quickly respond to the IoT affects on the consumers. To mitigate the excessive data collection, the officials will work as part of a diverse team to provide the companies with data collection frameworks. This diverse team composed of officials, privacy lawyers and data researchers will be in charge of creating data collection frameworks and policies that can be used by IoT manufacturers. These data collection frameworks will help restrict data collection to an as-needed basis and penalties heavily those who do not comply with this framework. Companies today should follow the 'Privacy Act', but they won't fully comply unless officials are intervening to ensure that this act is respected. For the officials, this is time-consuming because they must investigate the Privacy Act to narrow down the violations. They also have to partially rely on the public to inform them when a company might be breaking this act. So having some established data collection frameworks and policies will help the officials narrow down these potential violations. Additionally, this framework can provide clarity to the consumers about their data privacy rights because a normal consumer without any legal background will have a difficult time understanding the lengthy and jargon-filled Privacy Act.

When it comes to anonymity, the framework can emphasise on how to ensure the highest sensitive data like that related to health or smart homes remain anonymous. For this reason, the collaboration between data security researchers and officials to create the frame is important. The data security researchers are skilled in the domain of data extraction and will be able to provide insight into how companies can lower the chances of de-anonymising sensitive data. Together they will be able to create a framework that the companies can use to standardised the method they use to anonymise the IoT retrieved data instead of leaving it to the companies to figure out how to do so. Although there are other ways to mitigate IoT's privacy issues, this solution of having a collaborative framework between data security researchers, government officials and privacy lawyers will limit the excessive and de-anonymous collection of data.

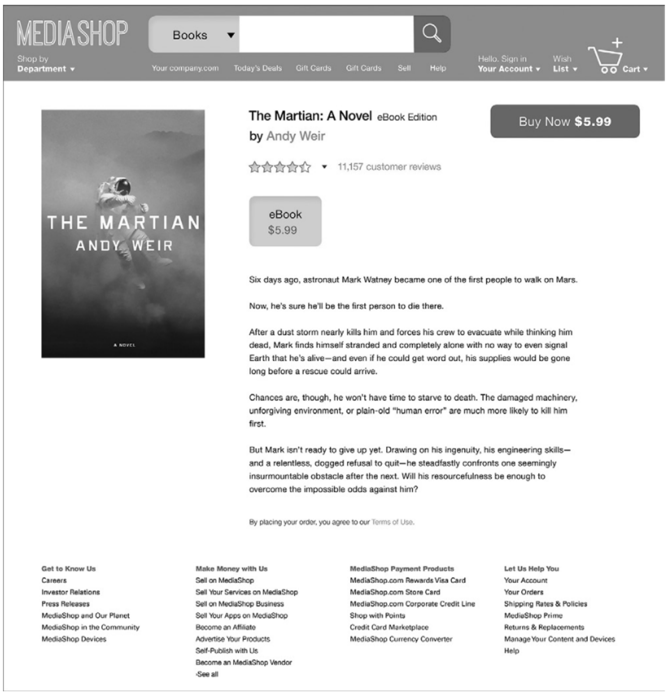
Following privacy's issues, one of IoT's security concern is securing this data from 3rd party which can be mitigated by decoupling and standardising the way IoT's shares and uses the data. It is suggested in *"Network-Level Security and Privacy Control for Smart-Home IoT devices: Network-Level Defense"* that rather than using 'device-level security' to implement 'network-level security'. Network-level security in this journal means to partially implement the security on the cloud and rollout continuous security maintenance patches. This security structure consists of three components. The first component is the IoT devices which has to constantly connect to the cloud to fetch security patches and updates. But to connect to the cloud, the manufacturers' will need to work with security service providers to create an API for these IoT to receive and send calls to. The second component is just that, it relies on using 'security-as-a-service'. These are security companies with skilled security employees who will provide the secured API to work with the IoT and the cloud. And lastly, the final component is the manufacturers who will be responsible for customising their products to meet the consumer's need but with fewer worries about how to implement the security. The main benefit of this additional layer of security is that when the security providers find a vulnerability, they will be able to immediately push out a patch onto the cloud where the IoT will auto-update hence keeping the devices updated and secure. Whilst this is happening, the manufacturers could continue to innovate and create new products because the security teams are handling these possible issues.

The next security issue revolving the implementation of security on IoT's limited hardware can be mitigated by changing the implementation to some lower resource usage protocols such as CoAP. In *"IoT Privacy and Security Challenges for Smart Home Environments"* mentions that "CoAP is an HTTP-like application layer protocol designed for constrained device networks" (Sivaraman et al., 2015). A major change between using this protocol versus the usual protocols used on our laptop for example is that CoAP uses User Datagram Protocol(UDP) rather than Transmission Control Protocol (TCP). So instead of establishing a connection each time the data needs to be sent, with UDP, the data packages are checked then sent. This helps reduces the overhead of using the IoT’s resources to set up the connection between the device and server for example. Devices like our computer will use ‘Transport Layer Security’ to encrypt the data before transmitting it. But, the resources it takes to run such operation is heavy. So what CoAP uses instead is ‘Data Transport Layer Security’ as a way to encrypt the datagram packages. The journal also states that “To secure communications, CoAP employs Datagram Transport Layer Security(DTLS). DTLS offers the same security services that TLS provides.” So by changing the protocol, we can provide a higher level of security rather than using a resource-intensive TCP protocol or implementing minimum security due to hardware limitations.

Figures from “*The End of Ownership: Personal Property in the Digital Economy*”

Figure 1: MediaShop Prototype

(Perzanowski & Schultz, 2016, p.91)



The Martian: A Novel eBook Edition
by Andy Weir

Six days ago, astronaut Mark Watney became one of the first people to walk on Mars.

Now, he’s sure he’ll be the first person to die there.

After a dust storm nearly kills him and forces his crew to evacuate while thinking him dead, Mark finds himself stranded and completely alone with no way to even signal Earth that he’s alive—and even if he could get word out, his supplies would be gone long before a rescue could arrive.

Chances are, though, he won’t have time to starve to death. The damaged machinery, unforgiving environment, or plain-old “human error” are much more likely to kill him first.

But Mark isn’t ready to give up yet. Drawing on his ingenuity, his engineering skills—and a relentless, dogged refusal to quit—he steadfastly confronts one seemingly insurmountable obstacle after the next. Will his resourcefulness be enough to overcome the impossible odds against him?

By placing your order, you agree to our Terms of Use.

Figure 5.1
An example of a MediaShop product page

Figure 2: Survey Results of Rights using the "Buy Now"

(Perzanowski & Schultz, 2016, p.92)

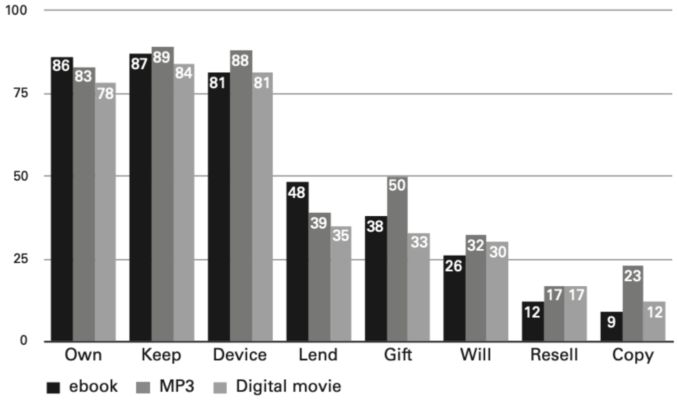
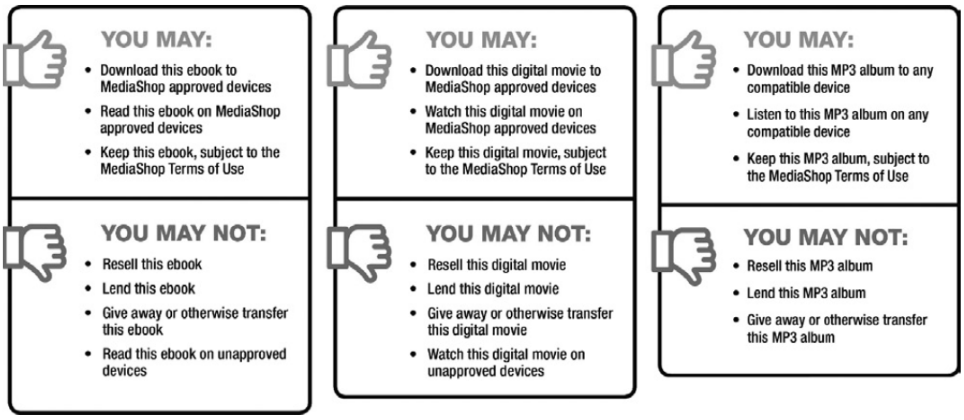


Figure 5.2
Percentage of respondents who believe the "Buy Now" button confers rights

Figure 3: Short Notices that can be used instead of "Buy Now"

(Perzanowski & Schultz, 2016, p.99)



YOU MAY:
- Download this ebook to MediaShop approved devices
- Read this ebook on MediaShop approved devices
- Keep this ebook, subject to the MediaShop Terms of Use

YOU MAY NOT:
- Resell this ebook
- Lend this ebook
- Give away or otherwise transfer this ebook
- Read this ebook on unapproved devices

YOU MAY:
- Download this digital movie to MediaShop approved devices
- Watch this digital movie on MediaShop approved devices
- Keep this digital movie, subject to the MediaShop Terms of Use

YOU MAY NOT:
- Resell this digital movie
- Lend this digital movie
- Give away or otherwise transfer this digital movie
- Watch this digital movie on unapproved devices

YOU MAY:
- Download this MP3 album to any compatible device
- Listen to this MP3 album on any compatible device
- Keep this MP3 album, subject to the MediaShop Terms of Use

YOU MAY NOT:
- Resell this MP3 album
- Lend this MP3 album
- Give away or otherwise transfer this MP3 album

Figure 5.4
Examples of MediaShop short notices

Figure 4: Survey Results of Rights using the Short Notice

(Perzanowski & Schultz, 2016, p.100)

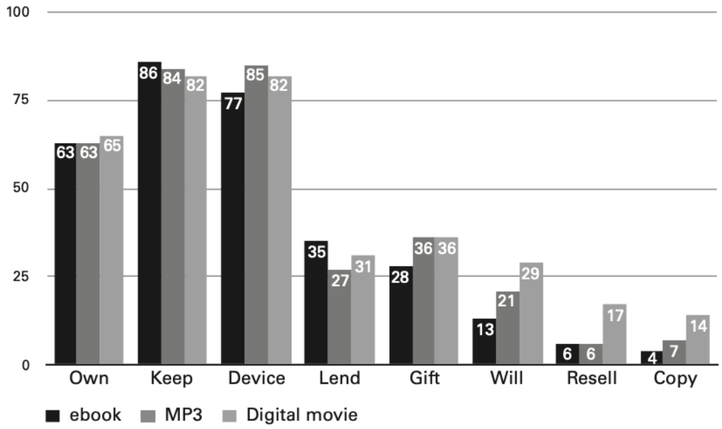


Figure 5.5
Percentage of respondents who believe the short notice confers rights

Finally, the last mitigation discussed will help resolve IoT's ownership issues. In the book, *"The End of Ownership: Personal Property in the Digital Economy"*, the authors created with an experiment to get a clearer understanding of what consumers think they are receiving as rights when they hit the 'Buy Now' button for digital purchases concerning ebooks, audios and digital movies on their prototype MediaShop site [Figure 1] which has a similar interface to Amazon. In the first experiment [Figure 2], the survey results show that a high number of consumers believe that they own the purchase, that they are allowed to keep it as long as they want and that they should be able to play it on the device of their choosing but there's a variation depending on what sort of media it is. However, a low number of consumers believe that they are allowed to make copies, resell, gift, leave their purchase as part of their will and lend their digital purchases. But in the second experiment [Figure 3], the MediaShop included short notices instead of a simple 'Buy Now' which indicated what the consumers may do with this purchase and may not do with this purchase. Consequently, as a result [Figure 4], these short notices helped the consumers be more consistent and confident in answering the survey about their rights associated with their purchase. There's less ambiguity of their rights between the different digital goods as well. This provides us with a good prototype of how we can implement digital purchases. Instead of just using the traditional ‘Buy Now’ buttons, we can provide short notices or use other buttons such as ‘Rent’ and ’Own’ to bring awareness to the consumer that this digital purchase is different from physical purchase in terms of rights gained. The current use of ‘Buy Now’ is misleading with digital purchases because it can be seen as the full rights that you gain when you buy something physically which includes the ability to resell, lend, and using the good on whatever device you choose. But looking at Apple’s ebooks which can only be played on Apple devices or Apple’s TV library where you can only play the shows on Apple devices, this is not the case (Perzanowski & Schultz, 2016, p.93). Similarly to the privacy issues mitigation, having a standardisation for the short notices and using different notions to distinguish between the typical ‘Buy Now’ can, as shown in the MediaShop prototype experiment, clarify confusions related to their ownership of the digital product.

As we mentioned beforehand IoT consists of both physical and digital ownership, where the physical ownership is associated with the hardware and the digital ownership is associated with the consumer’s data and the software embedded in the IoT. Now, the issue is how to distinguish what an IoT owner’s right is versus the Intellectual Property owner’s right. The mitigation for this issue can be found in understanding two particular property laws known as ‘Personal Property’ and ‘Intellectual Property(IP)’ laws.

Wikipedia defines personal property as “a property that is movable” (Wikipedia Contributors, 2020b). The *“The End of Ownership: Personal Property in the Digital Economy”* book mentions that “our personal property rules place a high value on alienability-the right of an owner of an item to resell it, give it away, or otherwise transfer it” (Perzanowski & Schultz, 2016, p.17). This personal property comes into play whenever you buy a physical good. You exchange a form of monetary value for the good and it becomes under your personal property. Although there may be contracts that limit your usage of the item upon your purchase, when you do sell the item, under the property law, the next owner doesn’t have to respect that limitation because the contract agreed upon was with you and the original seller.

The next key point is IP laws which is composed of multiple property laws such as patent law, trademark law, copyright law but our focus is copyright law. Wikipedia defines copyright as “a type of intellectual property that gives its owner the exclusive right to make copies of a creative work, usually for a limited time” (Wikipedia Contributors, 2019b). This law is tied in deeply with “the Exhaustion Principle”. The authors of the “*The End of Ownership: Personal Property in the Digital Economy”* denotes that “Exhaustion is the notation that an IP rights holder relinquishes some control over a product once it sells or given that product to a new owner”(Perzanowski & Schultz, 2016, p.12) The authors also note that it is this ‘Exhaustion Principle’ that was used to distinguish between intellectual and personal property rights when it came to ownership issues. The copyright law shouldn’t interfere with the personal property rights and based on the Copyright Act established in 1909 which still applicable today, it mentions that “nothing in this Act shall be deemed to forbid, prevent, or restrict the transfer of any copy of a copyrighted work the possession of which has been lawfully obtained.”(Perzanowski & Schultz, 2016, p.27) The main purpose of copyright law is to give an incentive for the creation of new works rather than to use this power to limit competition or restrict the consumer’s lawfully purchased goods.

The mitigation is then to keep these two laws distinct in digital purchases as it is the case for any physical purchases. There should be laws and policies in place so that the EULA licenses or any sort of license that the users have to agree to before using the product doesn’t interfere with personal ownership laws. If a user has lawfully purchased the digital good, they should be able to use it properly as an owner. If the item is to be rented or used as a subscription-only, as in the MediaShop example, it should be indicated before purchasing that this is for a license or limited time use. It should be illegal to sell a digital product with a ‘Buy Now’ tag and have the long-winded license that no one reads because of its length and jargon to define the consumer’s rights for the product. The digital goods should be regulated in at least two distinct categories of purchases: sales and licenses. If it’s a sale, then the implication is that you are allowed to what you like with it as with physical goods. If it’s a license, then the implication is that you do not own the item but are paying for permission to use it. Rather than using Digital Right Management (DRM) software or other means to break the digital product, the IP holders should consider what it means to sale a product to a consumer versus licensing the product to a consumer and adjust the pricing accordingly. IP holders need to realise cases such as the ones written on Wikipedia’s DRM that “The use of the DRM scheme in 2008's Spore backfired and there were protests, resulting in a considerable number of users seeking an unlicensed version instead. This backlash against the three-activation limit was a significant factor in Spore becoming the most pirated game in 2008, with TorrentFreak compiling a "top 10" list with Spore topping the list” (Wikipedia Contributors, 2019g). So the more IP holders try to implement some sort of DRM to limit the usage of legitimate purchase, the more consumers will turn to the alternative DRM-free copies. Besides on the same page, it mentions that “However, Tweakguides concluded that the presence of intrusive DRM does not appear to increase video game piracy, noting that other games on the list such as Call of Duty 4 and Assassin's Creed use DRM which has no install limits or online activation. Additionally, other video games that do use intrusive DRM such as BioShock, Crysis Warhead, and Mass Effect, do not appear on the list.” Consumers want to support the creation of new products but if it’s going to a headache to use the a lawfully purchased product, they will turn to alternatives.

After understanding this notion, we can discuss what this means about digital ownership with IoT and how it is mitigation for it. The data produced by the consumer’s IoT is part of their personal property. They have the right to consent to give the data to the IoT’s but it should be voluntary. The IP’s holders and manufacturers shouldn’t be allowed to break the IoT that they sold when the consumer decides not to give up their data. Similar to the analogue version of the IoT, there should be a law to assure that the digital IoT counterparts have basic functionality. For example, if you don’t give your consent for data collection for your IoT thermostat, it should still function as a thermostat but without the personalisation of it adjusting the temperature according to the number of people in the room. By having a minimum functionality requirement, the IoT that the consumers' purchase can be guaranteed to work. Similar policies like this can be implemented to assure that the personal property rights in IoT are respected. The other reason that it’s important to keep the distinction between a sale and a license is that the IoT are sold as a sale rather than as a license. So the consumer should have more ownership rights versus a license purchase. Even if the embedded software may be licensed, it shouldn’t hinder the personal rights associated with the IoT. For these reasons, the distinction between personal property and IP laws and that of a sale and a license is important to be regulated to ensure the consumer’s ownership of their IoT.

Conclusion

In conclusion, IoT are becoming more prevalent in our day to day lives. With the increase of IoT in each household, the issues that are associated with IoT which tend to be around privacy, security and ownership are in dire needed to be mitigated and resolved for the benefits of the current society and the future. As we discussed in this paper, the way to mitigate privacy issues related to excess data collection and anonymity being comprised is creating some standardised data collection frameworks that will be used by companies. In term of mitigating security issues, the solution is to let the security companies handle the creation of IoT’s API whilst the manufacturers supply them with the desired features and to implement security using lower resource-consuming protocols such as CoAP on IoT with hardware limitation. Finally, concerning mitigating ownership issues, the solution is to replace the ‘buy now’ buttons of digital purchases with short notices indicating the rights gained with the purchase and to standardise a minimum functionality requirement across different categories of IoT. Although these mitigations might seem time-consuming and costly upfront, they are just some example solutions that will help with the creation of more private, secure and ownership friendly IoT.

References

Apthorpe, N., Reisman, D., & Feamster, N. (2017). *Closing the Blinds: Four Strategies for Protecting Smart Home Privacy from Network Observers*. Princeton University's Computer Science Department. https://arxiv.org/pdf/1705.06809.pdf

Automatic. (2010). In *Oxford Dictionary of English*. Oxford University Press.

Barrett, B. (2019, June 30). *A Costly Reminder That You Don't Own Those Ebooks*. Wired. https://www.wired.com/story/microsoft-ebook-apocalypse-drm/

Bugeja, J., Jacobsson, A., & Davidsson, P. (2016). On Privacy and Security Challenges in Smart Connected Homes. *2016 European Intelligence and Security Informatics Conference (EISIC)*. https://doi.org/10.1109/EISIC.2016.21

Canada, O. of the P. C. of. (2018, March 20). *News release: Privacy Commissioner launches Facebook investigation*. Office of the Privacy Commissioner of Canada. https://priv.gc.ca/en/opc-news/news-and-announcements/2018/nr-c_180320/

Government of Canada. (2019, August 28). *Privacy Act (R.S.C., 1985, c. P-21)*. Justice Laws Website; Government of Canada. https://laws-lois.justice.gc.ca/ENG/ACTS/P-21/index.html

Lin, H., & Bergmann, N. (2016). IoT Privacy and Security Challenges for Smart Home Environments. *Information*, *7*(3), 44. https://doi.org/10.3390/info7030044

Ministère du Travail, de l'Emploi et de la Solidarité sociale. (2020, June 14). *P-39.1 - Act respecting the protection of personal information in the private sector*. Légis Québec; Les Publications du Québec Ministère du Travail, de l'Emploi et de la Solidarité sociale. http://legisquebec.gouv.qc.ca/en/ShowDoc/cs/P-39.1

Office of the Privacy Commissioner of Canada. (2018, January). *Summary of privacy laws in Canada - Office of the Privacy Commissioner of Canada*. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/

Ohlhausen, M. K. (2013, November 19). The Internet of Things: When Things Talk Among Themselves. *Federal Trade Commission*. https://www.ftc.gov/public-statements/2013/11/remarks-commissioner-maureen-k-ohlhausen-ftc-internet-things-workshop

Perzanowski, A., & Schultz, J. M. (2016). *The End of Ownership: Personal Property in the Digital Economy*. The Mit Press. (Original work published 2016)

Shouran, Z., Ashari, A., & Kuntoro, T. (2019). Internet of Things (IoT) of Smart Home: Privacy and Security. *International Journal of Computer Applications*, *182*(39), 3–8. https://doi.org/10.5120/ijca2019918450

Sivaraman, V., Gharakheili, H. H., Vishwanath, A., Boreli, R., & Mehani, O. (2015). Network-Level Security and Privacy Control for Smart-Home IoT Devices. *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE Xplore. https://doi.org/10.1109/wimob.2015.7347956

Wikipedia Contributors. (2019a, January 6). *Intellectual property*. Wikipedia; Wikimedia Foundation. https://en.wikipedia.org/wiki/Intellectual_property

Wikipedia Contributors. (2019b, February 7). *Copyright*. Wikipedia; Wikimedia Foundation. https://en.wikipedia.org/wiki/Copyright

Wikipedia Contributors. (2019c, February 26). *Privacy*. Wikipedia; Wikimedia Foundation. https://en.wikipedia.org/wiki/Privacy

Wikipedia Contributors. (2019d, March 4). *Big data*. Wikipedia; Wikimedia Foundation. https://en.wikipedia.org/wiki/Big_data

Wikipedia Contributors. (2019e, March 16). *Internet of things*. Wikipedia; Wikimedia Foundation. https://en.wikipedia.org/wiki/Internet_of_Things

Wikipedia Contributors. (2019f, August 26). *Smart home technology*. Wikipedia; Wikimedia Foundation. https://en.wikipedia.org/wiki/Smart_home_technology

Wikipedia Contributors. (2019g, October 22). *Digital rights management*. Wikipedia; Wikimedia Foundation. https://en.wikipedia.org/wiki/Digital_rights_management

Wikipedia Contributors. (2020a, March 5). *Ownership*. Wikipedia. https://en.wikipedia.org/wiki/Ownership

Wikipedia Contributors. (2020b, November 30). *Personal property*. Wikipedia. https://en.wikipedia.org/wiki/Personal_property

Wikipedia Contributors. (2020c, December 8). *De-identification*. Wikipedia. https://en.wikipedia.org/wiki/De-identification

Zeng, E., Mare, S., Roesner, F., & Allen, P. (2017). End User Security and Privacy Concerns with Smart Homes. In *Thirteenth Symposium on Usable Privacy and Security* (pp. 65–80). USENIX Association. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng

Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 1–20. https://doi.org/10.1145/3274469

Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2019). The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. *IEEE Internet of Things Journal*, *6*(2), 1606–1616. https://doi.org/10.1109/jiot.2018.2847733