Internet of Things Devices: Convenience, But at What Cost?

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Ranjodh Singh Sandhu

Spring 2021

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor
Kathryn A. Neeley, Associate Professor of STS, Department of Engineering and Society

Introduction

The Internet of Things (IoT) is exactly what it sounds like: a network of many different devices or *things* that can communicate with one another. Currently, the most common examples of IoT devices include the Amazon Echo and Google Home. Internet of Things devices are growing in use amongst households where they provide a new level of convenience for users. People are able to control household devices through voice commands as well as access a wide variety of features through the Internet. Many people, however, do not understand the full capabilities of IoT devices or the information that they record in order to provide the convenient features that are advertised. The implementation of IoT devices has "intersects with existing moral concepts like informed consent" (Allhoff & Henschke, 2018, n.p.). There are many sensors integrated in the devices that record information and communicate it across a network. Oftentimes, the information that is being stored and transferred is not clearly communicated or expressed in a way where the user fully understands (Zoonen, 2016, n.p.).

Due to the current lack of understanding of these advanced technologies, in both the regulatory and user dimensions, there is room for the Internet of Things to be misused. IoT devices can invade the privacy of the users by recording more information than the users are led to believe (Dolan et al., 2020, n.p.). In addition, the companies behind these IoT devices can use the data in ways that users are unaware of. In turn, people's privacy can be compromised without them even knowing (Elmaghraby & Losavio, 2014, n.p.). If regulatory laws are not updated as technology grows, it is possible that this uninformed surveillance can be happening legally (Hadyuk, 2016, n.p.). Analyzing the relationship between technology and government can help resolve the issues of regulation. In this paper, I argue that by focusing on educating the government about various technologies (such as IoT), decision-makers can effectively engage in practices that will allow society to benefit from the application of the technologies. This increased understanding can alleviate privacy concerns and enable ethically correct practices with improved regulation. Through better implementation and usage of technology, the benefits the innovations provide can be leveraged to benefit society. The remainder of this paper highlights the value of user privacy and how it is at risk as well as the application of Actor Network Theory and the Framework of Attitudes Towards Technology in Theory and Practice in this context. Actor network theory can be used to understand the risks of privacy invasion and how it could impact citizens' attitude towards IoT devices.

Problem Definition: The Value of User Privacy

User privacy has been a very controversial topic in the world of technology. It has been observed that there are two main reactions to the growing use of technology and the way it has impacted people's privacy. On one hand, there are people (mostly in the IT industry and R&D) that believe "we have zero privacy in the digital age and that there is no way we can protect it, so we should get used to the new world and get over it… The other reaction is that our privacy is more important than ever and that we can and we must attempt to protect it" (Van den Hoven et al., 2019, n.p.).

Over the years, it has become apparent that government policy has been reactive when dealing with technology. Steve Haro, a government affairs consultant and a former assistant secretary of commerce, recently stated in a discussion that "we still have questions to answer how to deal with technology dominance. We are not there yet because, unfortunately, Congress, for the most part, tends to act in response to crisis" (Triginelli, 2021, n.p.). Similarly, a former chief of staff claimed that another breach of data privacy may be needed to push Congress out of their reactive nature and spurn a major legislative move (Triginelli, 2021, n.p.). The extensive bureaucratic processes that have to be followed in the government make it ineffective in terms of regulation. Technology has consistently been outpacing law, which has opened up loopholes for people to exploit. Aside from the lawmaking process, the government is usually behind because officials are not up-to-speed with current technologies and safe practices. An example of this is the 2018 hearing where Mark Zuckerberg, the CEO and founder of Facebook fielded questions from senators about his company. The technological illiteracy of the officials was highlighted through the questions they asked. For example, Mark Zuckerberg was asked by Senator Brian Schatz "whether Facebook could see emails he sends on WhatsApp, which Facebook owns" (Stewart, 2018, n.p.). The problem with a question like this comes down to the fundamental fact that one does not send emails on WhatsApp. While this example focuses on Facebook's misconduct, it also highlights the issue that the people that are elected to influence decisions and make laws do not have knowledge on what they are regulating. The fact that the officials are asking these types of questions shows that they do not have a solid understanding of the technology that they are trusted to govern. In turn, companies may not take them as seriously and citizens may not have as much confidence in the government's abilities.

This lack of knowledge that has resulted in a slow-paced regulatory body is enabling vulnerabilities to exist in technology. With vulnerabilities comes the opportunity exploit. Those exploits being publicized have resulted in a negative stigma around technology. An example of an All three of these parts create a feedback cycle that stunts technological growth that could be used to help more people. The application of many Internet of Things devices can result in smart cities where citizens can enjoy convenience. However, with a large-scale implementation comes much risk. People's privacy would be at a large risk. Breaches could result from carelessness or from lack of knowledge on safe practices. Government officials could unintentionally allow attackers to access the systems through phishing or other means (Pasha, 2020, n.p.). The reason that this is important is that it is obvious that knowledgeable professionals can be hired to implement the system, but it is the officials and other government workers that will be maintaining it and using it. In a system like a smart city, there are many devices connected and "the more things that are connected, the greater the opportunity for cyberattackers to infiltrate [the] systems, exfiltrate sensitive data and disrupt potentially critical systems used in law enforcement, public health and other municipal applications" (Pasha, 2020, n.p.). The system is only as strong as its weakest link, which is the human element in this case. In order for the government to leverage the newest, most efficient technologies that can help society, it is clear that the current human practices must be altered to ensure safety.

Another aspect of the issue with privacy stems from the privacy policies themselves. They are known to be unclear and hard for users to follow. Typically, users are unaware of what data is being recorded and how it is being used. Similarly, they are uninformed of the capabilities of the technologies they are using and what is actually occurring. For example, many users have begun implementing IoT devices into their houses to create *smart homes*. If a network-connected coffee maker were to be activated twice on a Friday morning when it usually gets used once or if the smart shower head displays more activity than usual, is it possible that the user has someone who spent the night? Or if this occurs on routine, does that convey more about the user's personal life (Allhoff & Henschke, 2018, n.p.)? Seemingly harmless information can be aggregated to produce profiles on users and that same information could potentially be accessed by hackers or the manufacturers themselves. These habits that are being recorded can "reveal deeply intimate aspects of a person's life like being pregnant" (Allhoff & Henschke, 2018, n.p.).

Privacy policies tend to focus on consent instead of informed consent. Consent should not be defined as an affirmative response, because "stakeholders need to know what they are assenting to, and the 'informed' part adds that component" (Allhoff & Henschke, 2018, n.p.). Many users do not understand the wordy, lengthy privacy statements that they are required to acknowledge so they simply click accept. This legally clears the company to where they are not held liable but in reality, the user is not informed of what is occurring due to the impractical presentation of the information. The concept of ambiguity has played a large role in the extent of how informed users are. Through ambiguity, companies are able to develop loopholes in their privacy policies and leave the user relying on assumptions. Without clear statements that indicate the company's actual practices, "privacy policies are, in effect, meaningless… and they would provide declarations that would be unenforceable" (Reidenberg et al., 2016, n.p.). In other words, they could make claims that cannot be verified.

It is unclear what the motivations are behind the unclear privacy policies that companies use. In addition, there is uncertainty behind whether the companies even follow exactly what they have claimed in their privacy policies as many users do not understand them and it is hard to monitor. While there is need for reform in the realm of business regulation, there is also a need for society to become more knowledgeable about technology. There is a large knowledge gap between technical professionals and the average person. Since technology is becoming increasingly prevalent in everyday life, it is crucial that people grow with it. With other aspects of life, such as health, many people spend time researching and understanding different concepts. While they may not be knowledgeable to the point where they can practice medicine or perform surgery, people have foundational knowledge on how to stay healthy. If this is possible, why can't people research how they can stay safe when using technology? It is not necessary for them to become experts, but it would be helpful for everyone if they knew how to observe safe practices.

The current practices that persist in the realm of privacy policies has impacted users and how they feel about technology as a whole. The mistrust that exists cannot always be attributed to the technology itself. The analysis of STS models such as Actor-Network Theory and "A Framework of Attitudes Towards Technology in Theory and Practice" can help illustrate how society has perceived technology and why people have certain attitudes towards technological growth. There has been much debate surrounding the ethics behind IoT devices and the STS models help frame it.

Methods: Framing the Ethics Behind the Controversy Surrounding IoT

The controversy surrounding IoT and technology in general can be illustrated by the Actor-Network Theory (ANT). The article "Using ANT to Analyze E-Government Implementation in Developing Countries" provides an analysis of the e-government implementation in developing countries. While the United States is not a developing country and IoT is not exactly e-government, many of the concepts highlighted in the paper can be applied to the United States. In addition, the successful implementation of IoT devices in a smart city can increase the stability and efficiency of almost any country.

Actor network theory (ANT) is a logical approach where everything in the world has a constantly evolving network of relationships (Stanforth, 2007, 35). It provides a theoretical and methodological way to observe how technology impacts society. In addition, it highlights that the implementation of systems is more political than technological. ANT has the potential to be useful in engineering practice because it can introduce new perspectives that may not have been otherwise considered and provide a solution that accounts for society's interests. Through the use of Actor-Network Theory in Stanforth's paper, it is apparent that the involved networks must be supporting e-government in order for it to be successful. Another factor that impacts the success of e-government is the reliance on control of the forces that are in the system. The force could be a person or a thing and can be societal or technical. The concept of power is redefined and is described as "a composition that is made by many and attributed to one. The notion of 'power' is a convenient way to summarize collective action, but it cannot explain what holds the collective action in place" (Stanforth, 2007, 39). In other words, the term power "can be used as an effect, but never as a cause" (Stanforth, 2007, 39).

The points highlighted in the paper about the ongoing relationship between technology and government can apply beyond developing countries. Technological innovation can be slowed down by political processes. In a large-scale application, such as a smart city full of IoT devices, it is crucial to address the hurdles in maintaining or improving the systems down the line before any damage is done. In order to effectively govern and regulate a smart city, officials would need to better understand the technology and capabilities of the devices. This includes both the potential benefits and potential risks of various cases that could arise.

This offshoot of ANT is used to help conceptualize power and how the cooperation that is used to enforce that power is maintained. It highlights the importance of communicating how innovations can be beneficial for others and leveraging that to make more progress. Having an independent local network that is effective will provide stakeholders a base of power. It also shows how system reform is very political and that the success of the technical innovation depends more on the involved actors rather than the technology itself. This means that everyone's concerns need to be considered and people must be educated on the technology in order for it to be successful.

Additionally, “A Framework of Attitudes Towards Technology in Theory and Practice” highlights another key aspect of the use of IoT devices (or any technological innovation) on a wide scale. The paper is “a first attempt to address the apparent gap in empirical and theoretical research on attitudes towards technology” (Kerschner & Ehlers, 2016, 140). It produces a framework for categorizing different attitudes towards technology to help scholars clearly define their meaning through one of the four main categories as shown in the figure 1: enthusiasm, determinism, romanticism, and scepticism.

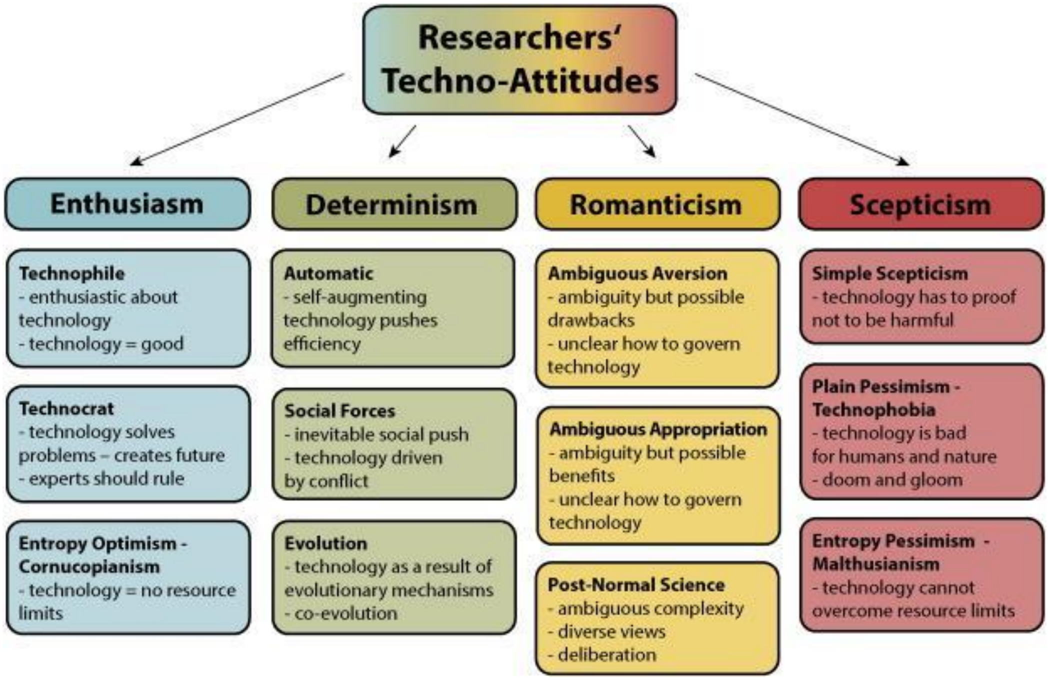

Researchers' Techno-Attitudes
Enthusiasm
Determinism
Romanticism
Scepticism
Technophile - enthusiastic about technology - technology = good
Technocrat - technology solves problems – creates future - experts should rule
Entropy Optimism - Cornucopianism - technology = no resource limits
Automatic - self-augmenting technology pushes efficiency
Social Forces - inevitable social push - technology driven by conflict
Evolution - technology as a result of evolutionary mechanisms - co-evolution
Ambiguous Aversion - ambiguity but possible drawbacks - unclear how to govern technology
Ambiguous Appropriation - ambiguity but possible benefits - unclear how to govern technology
Post-Normal Science - ambiguous complexity - diverse views - deliberation
Simple Scepticism - technology has to proof not to be harmful
Plain Pessimism - Technophobia - technology is bad for humans and nature - doom and gloom
Entropy Pessimism - Malthusianism - technology cannot overcome resource limits

Figure 1: A visualization of the spectrum of attitudes towards technology (Kerschner & Ehlers, 2016, 143)

As times have been changing, the attitude towards technology has shifted from that of confidence to one that is more varied. The issue with studying attitudes is that attitudes are subjective and research needs to be objective. This framework aims to provide an objective way to analyze people’s subjective views towards technology. With a system like a smart city that will impact many people, it is important to understand the reasoning behind these attitudes can help technology develop in a route that fosters more support for their implementation.

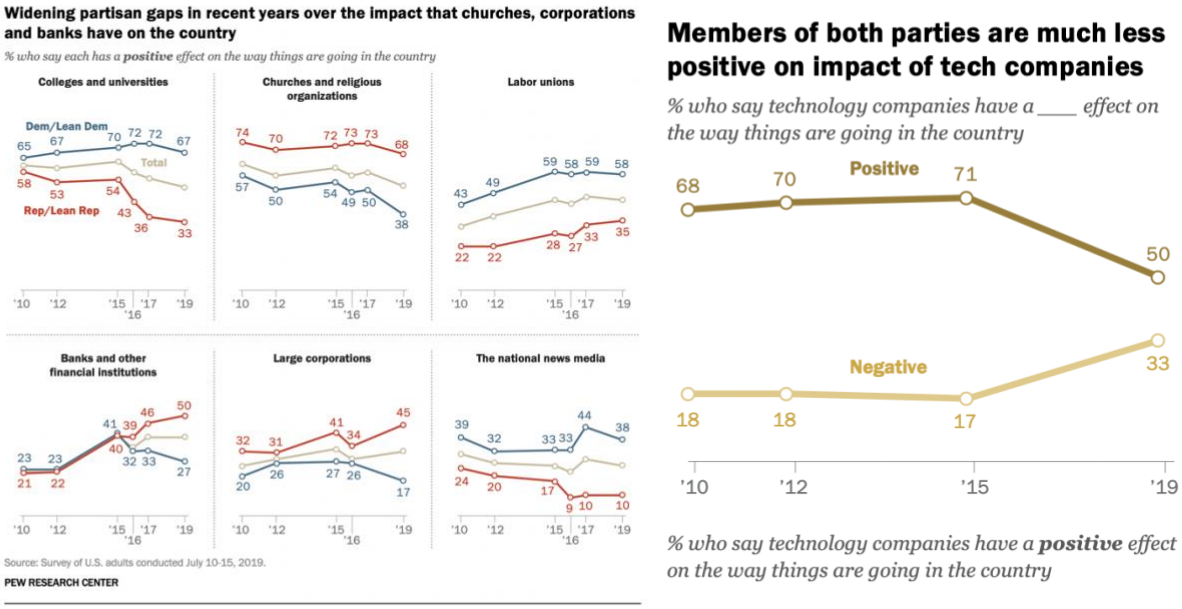
One of the biggest issues with using IoT devices on a wide scale is that people may be skeptical about how they are being used. Therefore, it is important to interact with citizens and potential users of IoT devices in smart cities to understand their specific concerns. From there, it will be easier to begin addressing those concerns and smoothing them out in order to gain support from people. The support, in turn, will create momentum and help make the project come to life. Implementing a smart city with various IoT devices without the support of citizens would create many more issues that could have been easily avoided. In addition, the reasoning behind the varied attitudes towards technologies may provide insight as to how improvements can be made across existing technologies.

A combination of the concepts illustrated in both “Using ANT to Analyze E-Government Implementation in Developing Countries” and “A Framework of Attitudes Towards Technology in Theory and Practice” can be used to understand the societal impact of the relationship between technology and government. It is clear that there needs to be communication flowing throughout the various stages of the development process in order for technological innovation to be successful. Objective data can be gathered from stakeholders through the framework introduced in “A Framework of Attitudes Towards Technology in Theory” in order to understand potential concerns of technologies in order to address them before implementation. The importance of focusing on the attitudes is to identify whether the issues that people have are ethical issues that have stemmed from the application of the technology in society. This will create a better relationship between technology, government, and citizens that mirrors the collectiveness highlighted in “Using ANT to Analyze E-Government Implementation in Developing Countries” to drive the success of innovations for society. Gathering data about the attitudes towards technology may highlight flaws that currently exist with sociotechnical systems. People may believe that they have an issue with the technology itself when in reality it is the application of the technology that they do not support.

Results: Good Intentions, Poor Execution

As presented in the paper, there are a lot of moving parts when it comes to implementing new technology (like IoT devices for a smart city) on a large scale. However, much of the inefficiency falls on the people involved with the technology, not the technology itself. From policymakers to users, there are improvements that need to be made on all facets of the system. Decision makers in positions of power often lack the knowledge required to understand the technology. This, paired with the slow-moving bureaucratic processes, makes it nearly impossible to keep up with current technology and regulate it effectively. As a result, if new technology is rolled-out, it is usually not governed correctly which leads to distrust in the government and technology as a whole. This opposition to technological growth poses as another hurdle. People are rightfully skeptical and distrusting of technology because of the stigma that has surrounded it through ineffective governing; however, this is not the fault of the technology itself but rather the companies implementing it and the government failing to regulate it. In other words, the intentions behind the technology and its application may mean well but there is backlash due to the way corporations have executed it for their own benefits.

As shown in figure 2 below, surveys by the Pew Research Center found that the percent of Americans surveyed that believe tech companies are positively impacting people dropped from 71% to 50% and the negative attitudes increased from 17% to 33% (Doherty & Kiley, 2019, n.p.). The survey was presented to many organizations and institutions to encompass a wide range of opinions. In addition, Kolakowski (2019) surveyed readers if they trusted Facebook after the aforementioned scandals occurred and found that 86% of respondents did not trust Facebook (n.p.). In another survey, when asked if big technology companies should be broken up, 44.2% of respondents said that they should (Kolakowski, 2019, n.p.). While this is not a majority, it is still a significant number and a good indicator that there is a lot of negative attitude towards technology companies that needs to be addressed.



Widening partisan gaps in recent years over the impact that churches, corporations and banks have on the country

*% who say each has a **positive** effect on the way things are going in the country*

Colleges and universities

Churches and religious organizations

Labor unions

Banks and other financial institutions

Large corporations

The national news media

Source: Survey of U.S. adults conducted July 10-15, 2019.

PEW RESEARCH CENTER

Members of both parties are much less positive on impact of tech companies

% who say technology companies have a ____ effect on the way things are going in the country

*% who say technology companies have a **positive** effect on the way things are going in the country*

Figure 2: A visualization of the shift in attitude towards technology (Doherty & Kiley, 2019, n.p.)

In a more recent survey conducted by Hyland, 1000 consumers in the United States were polled to understand how technology has played a role in their lives during the COVID-19 pandemic and how that has impacted their trust in technology (Sandle, 2021, n.p.). The results showed that 71% of respondents had increased their technology usage with 44% claiming that it had increased significantly. In terms of trust, 39% of respondents said they had little-to-no trust with smart speaker devices (Sandle, 2021, n.p.). This is significant as these smart speaker devices are IoT devices, which are necessary in a smart city system. When asked about artificial intelligence, 41% of respondents did not trust it. In addition, 57% of respondents thought that it would in fact do damage over the next 10 years (Sandle, 2021, n.p.).

It is clear that there are some issues with the way that technology is being applied by big tech companies. In order for technology usage to grow and be applied in a large scale, like a smart city, people need to support it and trust it. Instead of fearing the technology or advocating for bans, it would be more beneficial to push for regulation and restrictions. This, however, comes back to the issue of poor regulation by the government. Edelman's 2020 Trust Barometer found that 61% of people surveyed believe that the "government does not understand emerging technologies enough to regulate them effectively" (Nair, 2020, n.p.). In addition, the survey also found that 56% of people think that distrusted technologies should be regulated. This is significant as it shows that people may still be interested in the benefits that the technologies provide.

Through analyzing previous cases of unethical use of technology in society similar to those mentioned earlier, the current flow of technology can be simplified as shown in figure 3 below. The current structure of technological innovation and application, which includes the implementation of IoT devices, is shown in four steps. At the top, are the innovators. They are the developers and engineers that see a need and use for a product in society. It is assumed that they are developing the technology for ethical purposes, as indicated by the green arrow. After all, in order for a product to be successful, there needs to be a customer and use case. In addition, ethics courses and discussions are being integrated into many engineering curriculums to help create a future of ethical engineers. Next, comes the businesses and corporations as they are always looking for the latest technology. Sometimes, the innovators may be a part of those companies. They take the technology and use it for whatever application they need. Those businesses then create products or services that the consumers use, sometimes unknowingly. Since the technology is new, there may not be strong regulation in place which allows the companies to use that to their advantage. This is where the majority of the issues occur, indicated by the red arrow. At this point, a leak usually occurs that alerts the public of what is actually going on. This leads to the final step, the government. The government then reacts to the information and creates rules and regulations to address the concerns. The speed of development and integration in the private sector is too quick to where the government cannot keep up. Therefore, the government is seen as a reactive entity and gives time for companies to exploit loopholes. This is how the distrust in both technology and the government occurs.

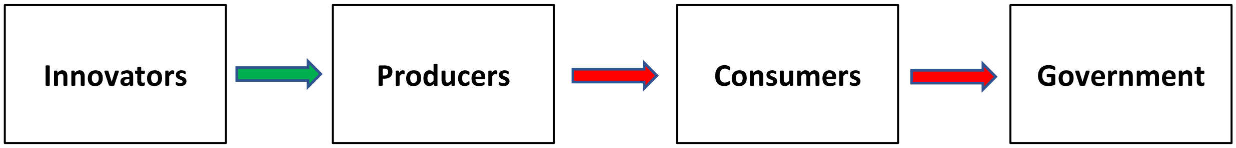


Figure 3: A visualization of the current structure of technological innovation and implementation

This model can be applied to the Internet of Things. For example, the technology was created as a means for various devices and sensors to communicate with one another over a network. The potential applications of IoT devices in smart cities could improve the infrastructure and management of cities as well as cut down on costs and pollution. In households, IoT devices have helped people who may not be as mobile carry out common tasks. It was not developed with the purpose to spy on users and collect their data unknowingly. Instead, that was a decision that producers made when they applied the technology into their products and created their complicated privacy policies. It was then rolled out to the consumers who got to enjoy the convenience that the technology was developed to provide, but at a cost they may not have been aware of. Allhoff & Henschke (2018) illustrated a strong example of the privacy issues through a “widely publicized case [where] Target mined a client's purchasing habits, predicted that she was pregnant, and [sent] a mailer promoting baby items to her home. As it turns out, she was still in high school and, while she was in fact pregnant, her family did not know; they literally found out because of the mailer" (n.p.). There is a high probability that the girl was not informed that her purchasing habits were being tracked and it was a clear misuse of her information. This is not the fault of the technology itself but the way it was applied.

To mitigate this, the model should be modified as shown in figure 4. If the government were to be quicker and more knowledgeable, it could move from the last step to the second step of the process. Through better understanding, the government could explore potential use cases to benefit society and create regulations from the start. This would then force companies and businesses to abide by the restrictions and ultimately benefit the consumers. The end consumers would have greater trust in both the government and the tech companies. In other words, focusing on the government could trickle down and solve the issues that occur in the other steps.

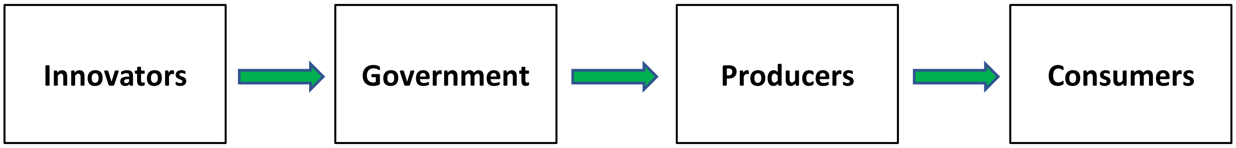


Figure 4: A visualization of the proposed structure of technological innovation and implementation

In the case of IoT devices, the government could review the technology and capabilities from the innovators themselves. As a regulatory body, the government can use its judgement after gaining a stronger understanding of the capabilities of IoT devices. This way, the government can regulate which data is necessary for the devices to function for their specific use cases. In addition, if the capabilities of IoT devices are communicated, the government can ensure that the data that is being collected is being used appropriately. This can address privacy concerns that users may have and restore confidence in the government and the technology. The government could even push for more clear privacy policies so that the consumers are aware of the information that is being tracked and how it is being used. At the same time, the government could explore potential large-scale use cases of IoT devices that could benefit society as a whole, such as smart cities. By focusing on the government and helping it understand and embrace technology instead of fearing it, can produce benefits that trickle down to the consumers and society as a whole. The government needs to lead by example and show that it is possible to create a balance of efficiency and privacy where everybody wins.

Conclusion

In this paper, I advocate for tighter regulation and an increase of knowledge surrounding technology. Through the use of Stanforth's "Using ANT to Analyze E-Government Implementation in Developing Countries" and Kerschner & Ehlers "A Framework of Attitudes Towards Technology in Theory," I argue that instead of focusing on increasing technological awareness across the government, producers, and consumers, many of the issues present in today's society surrounding IoT devices can be alleviated by focusing on improving regulation. By focusing on improving the government's understanding of technology, they can effectively regulate IoT and new innovations so that citizens can enjoy the benefits on a large scale.

Through better understanding and increased awareness, both the government and consumers can be less vulnerable to hidden unethical practices and demand a higher standard from technology companies. The current and potential users of the Internet of Things can have more insight into the actual usage of their data. Government officials can learn more about the benefits of these technologies as well as the main concerns that need to be addressed with regards to the implementation of the technology. In addition, policymakers can understand why having knowledge on these technologies is important and how it could impact society by attempting to keep up with the newest innovations. Through this stronger understanding, systems can be maintained more securely and can help the government gain trust of the citizens. The citizens of the potential smart cities can have a better understanding of both the benefits and concerns of integrating IoT devices and can feel more confident if the issues brought to light are addressed.

Oftentimes, it is unclear on where to start when trying to address the issue of consumer privacy and misuse of technology. It may seem obvious to focus on educating everyone as a whole, but this is not always practical. Through this research, it has become more apparent that focusing the efforts on increasing technical awareness in the government will create impacts that spread to both producers and consumers. The tighter regulation will inhibit exploitation of technology by the producer which will result in greater trust by consumers. Additionally, the increase in understanding by policymakers will lead to more public sector innovation that can be applied in large scale to increase efficiency and quality of life in society.

References

Allhoff, F., & Henschke, A. (2018). The Internet of Things: Foundational ethical issues. *Internet of Things, 1-2*, 55-66. doi:10.1016/j.iot.2018.08.005

Doherty, C., & Kiley, J. (2019, July 29). Americans have become much less positive about tech companies' impact on the U.S. Retrieved March 18, 2021, from https://www.pewresearch.org/fact-tank/2019/07/29/americans-have-become-much-less-positive-about-tech-companies-impact-on-the-u-s/

Dolan, A., Ray, I., & Majumdar, S. (2020). Proactively extracting IoT Device capabilities: An application to smart homes. *Data and Applications Security and Privacy XXXIV,* 42-63. doi:10.1007/978-3-030-49669-2_3

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in smart cities: Safety, security and privacy. *Journal of Advanced Research, 5*(4), 491-497. doi:10.1016/j.jare.2014.02.006

Hayduk, J. (2016, June 29). The other 2016 cycle: When technology outpaces policy. Retrieved October 21, 2020, from https://www.vox.com/2016/6/29/11978162/regulation-business-2016-cycle-technology-outpaces-policy

Kerschner, C., & Ehlers, M. (2016). A framework of attitudes towards technology in theory and practice. *Ecological Economics, 126*, 139-151. doi:10.1016/j.ecolecon.2016.02.010

Kolakowski, N. (2019, November 07). Americans losing trust in tech industry. Retrieved March 18, 2021, from https://insights.dice.com/2019/11/07/americans-losing-trust-tech-pew/

Nair, S. (2020, February 25). In technology we trust(ed). Retrieved March 18, 2021, from https://www.edelman.com/research/trend-eroding-trust-tech-continues

Pasha, Haider. (2020, March 26). This is how we secure smart cities - what leaders must consider. Retrieved October 20, 2020, from https://www.weforum.org/agenda/2020/03/this-is-how-we-secure-smart-cities/

Reidenberg, J. R., Bhatia, J., Breaux, T. D., & Norton, T. B. (2016). Ambiguity in privacy policies and the impact of regulation. *The Journal of Legal Studies, 45*(S2). doi:10.1086/688669

Sandle, T. (2021, March 03). As technology use grows, so do feelings of 'digital distrust'. Retrieved March 18, 2021, from http://www.digitaljournal.com/tech-and-science/technology/as-technology-use-grows-so-do-feelings-of-digital-distrust/article/586364

Stanforth, C. (2007). Using Actor-Network Theory to analyze e-Government implementation in developing countries. *Information Technologies and International Development, 3*(3), 35-60. doi:10.1162/itid.2007.3.3.35

Stewart, E. (2018, April 10). Lawmakers seem confused about what Facebook does - and how to fix it. Retrieved March 11, 2021, from https://www.vox.com/policy-and-politics/2018/4/10/17222062/mark-zuckerberg-testimony-graham-facebook-regulations

Triginelli, S. (2021, April 13). Government's reactive nature hobbling tech regulation, expert says. Retrieved May 08, 2021, from https://broadbandbreakfast.com/2021/04/governments-reactive-nature-hobbling-tech-regulation-expert-says/

Van den Hoven, J., Blaauw, M., Pieters, W., & Warnier, M. (2019, October 30). Privacy and information technology. Retrieved March 11, 2021, from https://plato.stanford.edu/archives/sum2020/entries/it-privacy/

Zoonen, L. V. (2016). Privacy concerns in smart cities. *Government Information Quarterly, 33*(3), 472-480. doi:10.1016/j.giq.2016.06.004