

# **THE EFFECT OF THE INTERNET OF THINGS ON CITIZENS' PRIVACY RIGHTS**

A Research Paper submitted to the Department of Engineering and Society  
In Partial Fulfillment of the Requirements for the Degree  
Bachelor of Science in Computer Science

By

Kajal Sheth

March 27, 2020

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

Catherine D. Baritaud, Department of Engineering and Society

## **TECHNOLOGICAL ADVACEMENTS IN THE UNITED STATES**

According to reports from the United Nations, around 68% of the population might live in urban areas by 2050 (2018) with the development of new technologies to facilitate living.

The technical portion of this project focuses on building a platform to fix problems within the community by building a bridge between the community members and city officials. The goal of this product is to ensure optimal living conditions and a safer future for the community.

This platform will allow community members to post blueprints about project ideas for improvements they wish to see around the city so when city officials take action to enhance the community, they know exactly what changes the citizens want. Tightly coupled with the technical project, the Science, Technology and Society (STS) research focuses on the privacy rights that are concerned with the Internet of Things (IoT). IoT is a system of interrelated computing devices in everyday objects that enable them to send and receive data (Patel, 2018). Smart cities have amazing living conditions, facilitated traffic, fast internet (Patel, 2018), and that is possible through means of IoT, having devices that can send data in real-time. However, the pros and cons of IoTs, which make them controversial, is that the data that gets collected is seen by many individuals as a violation of privacy. Some people feel strongly against the collection of personal data and would rather not have advanced assistive technology if that means none of their personal data gets collected. Using the Pacey's Triangle framework (Pacey, 1983) the STS research will investigate the effect on individual privacy rights by the IoTs installed for advancements in cities.

## HOW IS IOT HARMFUL TO OTHERS?

According to a survey done by the Pew Research Center, 81% of U.S. adults feel they have little or no control over how private sector technology companies use their personal information (Auxier, 2019). Technology has often been seen in a positive light since the first invention of the wheel in 3500 B.C. (Wolchover, 2012). Since then inventions have increased dramatically with the intent to encourage the growth of society. Though there are many innovations that facilitate day to day life, many current technologies that are part of individuals' everyday lives are collecting their data, violating their privacy. This is an important issue not only because often users are unaware of what technologies around them are monitoring them, but also because users do not know how to stop it. A survey by Consumers International and the Internet Society reported that though 63% of participants find monitoring technologies to be “creepy”, still almost 70% of them admitted to owning such technologies (Molla, 2019). This is because over time citizens have grown reliant on these technologies, and blindly trust the companies that manufactured them. There have been no previous laws moderating big technology companies so they continue manufacturing products that monitor their users, leaving users to be manipulated. While innovators are saying they want to advance and better society, lawmakers must first take a step back and ensure users are not being harmed in the process. Otherwise, instead of taking one step forward society would be taking ten steps backwards. This STS research paper will discuss the severity of the effects of IoT on society.

## VULNERABILITY OF SOCIETY

There are countless examples of technologies that are unknown to users, manipulating them. Google is arguably one of the most well-known brands in the world. Google has well-built credibility so it is trusted by many users, being the most popular multi-platform website with over 250.5 million visitors in 2019 (Clement, 2020). Google has a variety of projects and one of its software is called Google Assistant, which is an artificial intelligence software primarily available on mobile and smart home devices. In April 2018 it was discovered owners of Google Assistant had their voices recorded and kept, all without their knowledge (Fussel, 2019). This is a prime example of a big technology company taking advantage of its users because nobody knows what those voice recordings were used for and who had access to them, and that is very dangerous.

Along with individual privacy rights being at risk, without secure technology the nation as a whole can be at risk too. Figure 1 below shows a heat map from Strava, a popular fitness tracking application. Strava leaked a heat map in November 2017, exposing



Figure 1: Strava Heat Map: This is a heat map realized from the application Strava, which is a snapshot of a map made from collecting individual GPS points. This map is of a military base in Helmand Province, Afghanistan with the routes taken by joggers that are highlighted through Strava (Hern, 2018).

more than 3 million users' locations, including users who were in remote military bases in Iran (Hern, 2018). On top of arguing with the media that the leak of confidential information was not the company's fault, Strava

proclaimed it was the users who did not understand the privacy concerns. However, the reality is that this was a significant breach of privacy to their users, Strava had no right to release these maps, and many people's lives could have been at risk. If the legislative system had put restrictions on technology companies from the beginning, these products would be more secure.

## **PRIVACY RIGHTS**

In the United States, there are no federal laws that address social media privacy rights. The closest thing that has taken place is the California Consumer Privacy Act (CCPA) that was passed on June 28th, 2018. The CCPA puts restrictions on how companies use and collect data. It gives citizens the right to know what personal data is being collected about them, where and to whom their personal data is sold or disclosed the ability to say no to the sale of their data, and access their personal data ("California Consumer Privacy Act", n.d.). This was a huge landmark, changing the power gears into the hands of the user. However, there is no federal legislation nor any other state that has released legislation pertaining to this issue so while users in California are safe, the same cannot be said for other states. This is a very good beginning to exemplify the change that needs to happen but it is nowhere near the end result that we need. Legislation like the CCPA can only spread to other states or the federal government when enough people talk and demand changes. Citizens now more than ever must recognize and voice their opinions of the injustice that is happening so that they can fight and win for the protection of their rights.

## **SOCIETAL IMPACT**

With the correct measures taken, there can be advancement in society without jeopardizing citizen's rights. The Pacey's Triangle framework can be used to identify

relationships between the larger network of people who will impact or be impacted by adaptation of IoT. Pacey's Triangle organizes a technology into its stakeholders from three main components: organizational, cultural, and technological, as depicted below in Figure 2. While IoT sits in the center as the technology we will focus on, for the technological sector of the triangle the directly impacted stakeholders will be engineers. Engineers are the ones

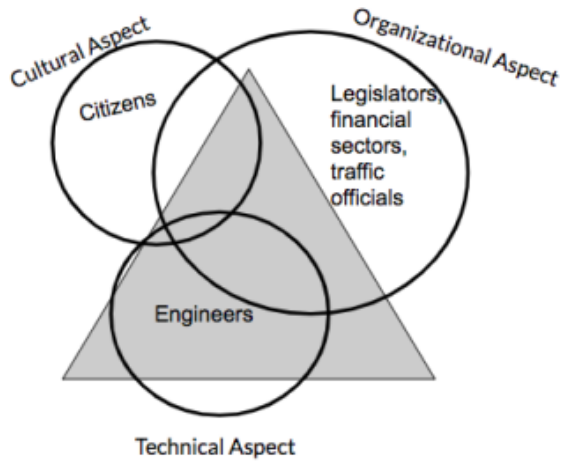


Figure 2: Pacey's Triangle for the Effect of the Internet of Things on Society: An illustration of the three aspects from Pacey's (adapted by Sheth from Pacey, 1983, p.6).

building the technologies that make up the IoT system. The engineers create tools like sensors and cameras to mandate traffic and are in charge of maintaining the technology created to collect accurate data. Along with creating technology, engineers will be going through the data collected to derive patterns and conclusions and pass on that information to the government so that they can make

appropriate changes based on this data. This explains the overlap between the technological sector and the organizational sector as shown in Figure 2.

The organizational sector of the triangle for IoT includes legislative bodies of the government, financial sectors, traffic officials, and those administrative roles that would be affected with advancements in technology. From an organizational perspective, the financial sectors and traffic officials will be very happy with the adoption of IoT because it would facilitate their jobs. In theory, organizational stakeholders would like this because this would facilitate their work, having quicker access to data to fix whatever problems

may arise. However, for legislative bodies, due to the controversy on the issues from the opinions of the citizens that inhabit a community, it would be a stressful task.

In the cultural sector, from an ethical viewpoint, are the citizens being impacted by IoT. The citizens can see IoT in one of two lights: either positive as a means to live day by day or negative due to violation of citizens' privacy rights through the collection of real time data for potential future use. An example of positive impact of IoT is the smart technology built in South Korea built to solve their problems such as water meters. The product ensures real time water updates as mentioned before. IoT can also be viewed negatively. The cultural sector has a big overlap with the organizational sector because the legislator's decisions have a direct impact on them. If legislators make no law to warn companies to regulate or limit the data they collect from users, then essentially these big technology companies are indestructible, with the ability to cause grave harm to the user, as was the case with Strava application almost leaking user's locations (Hern, 2018). On the other hand, if legislator's do pass a law that would restrict the data that gets collected, that would make citizens feel safer with the use of IoT software, and more willing to accept it as a part of the growth of technology. However, there needs to be some middle ground met from both sides and that is the difficult part to overcome: exactly what amount of regulation is the right amount? There is barely any overlap between the technology sector and cultural sector because though the technology is collected and data is analyzed by engineers, citizens get more directly impacted by the organizational sector.

## **PROTECTION THROUGH NEW LEGISLATION**

Through the research conducted on the effect of IoT on the community through different factors like cultural, organization, and technology, while also weighing where privacy rights fall in between all of these, and how significantly they will be affected, I hope to find out the next steps to create guidelines or understanding of how cities and communities can have IoT and advance, forming solutions to problems without jeopardizing their rights or safety.

If legislators make no law to warn companies to regulate or limit the data they collect from users, the companies become indestructible. Without proper administration over companies' users can end up harmed as was the case with Strava (Hern, 2018) or Facebook's voice memos being recorded unknowingly (Fussel, 2019). If legislators do pass a law that would restrict the data that gets collected, that would make citizens feel safer with the use of IoT software, and more willing to accept it as a part of the growth of technology. Thus, there needs to be some middle ground met from both sides.

A good starting point in amending legislation that will ensure technology companies are controlled is to follow in the steps of the United Kingdom. On January 21, 2020 United Kingdom's Parliament passed the Age-Appropriate Design Code, a new privacy law requiring gaming applications, connected toys, social media, and other online networks, in particular those that can be used by users under the age of 18, to restrict how they handle users' personal information. The law also requires websites and applications to collect as little personal information from minors as possible (Singer, 2020). Discussion for the approval of this legislation arose from social media websites proclaiming they are safe for the use of children however inappropriate advertisements and suggestions were still being displayed to children.



These applications and social media platforms that are causing concerns in the United Kingdom, are also widely used all around the world, including the United States. For example, in September 2019 Google agreed to pay \$170 million in fines to settle charges of YouTube violating children privacy concerns in the United States (Singer, 2020). The only difference is that seeing such cases, the United Kingdom took action, while the United States still has not. While the concerns over social media restrictions arose for different reasons between the two countries, the goal remains the same: to protect users' data. Knowing there is a history of rights being violated, which will only continue to grow, it would be a unjust to just sit and let citizens get manipulated. If citizens come together to show their concerns, Congress will feel pressured to realize the gravity of the problem at hand. Once there is legislation moderating technology companies, society can both continue to advance without making sacrifices.

## WORKS CITED

- 68% of the world population projected to live in urban areas by 2050. (2018, May 16). Retrieved from <https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html>
- Auxier, B. (2019, November 15). Americans and privacy: concerned, confused and feeling lack of control over their personal information. *Pew Research Center*. Retrieved from <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>
- California Consumer Privacy Act. (n.d.). Retrieved from <https://www.caprivacy.org/>.
- Clement, J. (2020, February 27). Most popular U.S. multi-platform web properties 2020. Retrieved from <https://www.statista.com/statistics/271412/most-visited-us-web-properties-based-on-number-of-visitors/>
- Fussell, S. (2019, August 15). People are starting to realize how voice assistants actually work. *The Atlantic*. Retrieved from <https://www.theatlantic.com/technology/archive/2019/08/facebook-paid-contractors-listen-messenger-audio/596143/>
- Hern, A. (2018, January 28). Fitness tracking app Strava gives away location of secret US army bases. *The Guardian*. Retrieved from <https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases>.
- Molla, R. (2019, May 13). People say they care about privacy but they continue to buy devices that can spy on them. Retrieved from <https://www.vox.com/recode/2019/5/13/18547235/trust-smart-devices-privacy-security>
- Pacey, A. (1983). *The culture of technology*. Cambridge, MA: MIT Press.
- Patel, C., & Doshi, N. (2018). IoT: An overview. *Internet of Things Security*, 1–59.

Singer, N. (2020, January 22). Britain plans vast privacy protections for children. *The New York Times*. Retrieved from <https://www.nytimes.com/2020/01/21/business/britain-children-privacy-protection-kids-online.html?searchResultPosition=3>

Wolchover, N. (2012, March 02). Why it took so long to invent the wheel. Retrieved from <https://www.livescience.com/18808-invention-wheel.html>

## BIBLIOGRAPHY

- 68% of the world population projected to live in urban areas by 2050. (2018, May 16). Retrieved from <https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html>
- Auxier, B. (2019, November 15). Americans and privacy: concerned, confused and feeling lack of control over their personal information. *Pew Research Center*. Retrieved from <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>
- Bargmann, J., Keaveny, T., O'Hare, E., & Weyrich, M. (2018, November 28). YOU Issue: Charlottesville leads in income inequality. *VILLE Weekly*. Retrieved from <https://www.c-ville.com/income-inequality/> )
- Boston smart city playbook. (n.d.). Retrieved from <https://monum.github.io/playbook/#play1>
- Bowerman, B., Braverman, J., Taylor, J. Wimmersperg, U. (2000, September 28). The vision of a smart city. Retrieved from <https://www.osti.gov/biblio/773961>
- Cagliano, A.C., Mangano, G., Marco, A. D., Neirotti, P., & Scorrano, F. (2014, January 19). Current trends in Smart city initiatives: Some stylised facts. *ScienceDirect*, 38, 25-36. <https://doi.org/10.1016/j.cities.2013.12.010>
- California Consumer Privacy Act. (n.d.). Retrieved from <https://www.caprivacy.org/>.
- Cho, M.H. (2019, January 17). South Korea's IoT in full swing: From water meters to AI-powered smart buildings. Retrieved from <https://www.zdnet.com/article/south-korea-iot-in-full-swing-from-water-meters-to-ai-powered-smart-buildings/>.
- Citizen engagement is key to smart city success. (2018, March 8). *SmartCitiesWorld*. Retrieved from <https://www.smartcitiesworld.net/news/news/citizen-engagement-is-key-to-smart-city-success-2685>

- Clement, J. (2020, February 27). Most popular U.S. multi-platform web properties 2020. Retrieved from <https://www.statista.com/statistics/271412/most-visited-us-web-properties-based-on-number-of-visitors/>
- Fussell, S. (2019, August 15). People are starting to realize how voice assistants actually work. *The Atlantic*. Retrieved from <https://www.theatlantic.com/technology/archive/2019/08/facebook-paid-contractors-listen-messenger-audio/596143/>
- Hern, A. (2018, January 28). Fitness tracking app Strava gives away location of secret US army bases. *The Guardian*. Retrieved from <https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases>
- Kitchin, R. (2013, November 29). The real-time city? Big data and smart urbanism. *SpringLink*, 79, 1-14. <https://doi.org/10.1007/s10708-013-9516-8>
- Lee, J.H., Lee, S.H., & Phaal, R. (2012, November 12). An integrated service-device-technology roadmap for Smart city development. *ScienceDirect*, 80, 286-306. <https://doi.org/10.1016/j.techfore.2012.09.020>
- Molla, R. (2019, May 13). People say they care about privacy but they continue to buy devices that can spy on them. Retrieved from <https://www.vox.com/recode/2019/5/13/18547235/trust-smart-devices-privacy-security>
- Pacey, A. (1983). *The culture of technology*. Cambridge, MA: MIT Press.
- Patel, C., & Doshi, N. (2018). IoT: An Overview. *Internet of Things Security*, 1–59.
- Rouse, M. (2019). *IoT Agenda*. Retrieved from <https://internetofthingsagenda.techtarget.com/definition/smart-city>
- Sanders, J. (2020, January 3). Facebook data privacy scandal: A cheat sheet. *TechRepublic*. Retrieved from <https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/>

Sidney Fussell. (2020). Retrieved from [https://everipedia.org/wiki/lang\\_en/sidney-fussell](https://everipedia.org/wiki/lang_en/sidney-fussell)

Singer, N. (2020, January 22). Britain plans vast privacy protections for children. *The New York Times*. Retrieved from <https://www.nytimes.com/2020/01/21/business/britain-children-privacy-protection-kids-online.html?searchResultPosition=3>

Singer, N. (2019, November 2). The government protects our food and cars. Why not our data? *The New York Times*. Retrieved from <https://www.nytimes.com/2019/11/02/sunday-review/data-protection-privacy.html>.

Wolchover, N. (2012, March 02). Why it took so long to invent the wheel. *LiveScience*. Retrieved from <https://www.livescience.com/18808-invention-wheel.html>

