

# Private Data in a World Where Everything is Public

HENRY WILT

Ursinus College  
hewilt@ursinus.edu

April 11, 2022

## Abstract

*In this Research Report, we will be talking about private data, how to keep it private, who should hold it, and what kinds of data should be held in a World that everything you have the internet will either be public or already is public information and access. This is an assignment for Human Computer Interaction[1], to write a research report on topic that deals with Human Computer Interaction. As this is a report on 5 different papers, we need to keep in mind the time when the author submitted these papers as the internet is a fast-paced place and always changing.*

## I. INTRODUCTION

THE world has changed from the start of the internet, at the start there was little done about privacy and security as the internet was used only for academic or government use. There was very little to no use of it to the general public. As time went on and the internet grew from government and academia use, the use of the internet increased from 2.6 million in 1990 to almost 2 billion in 2010 and now over 3.5 billion in 2016[2]. Over that time, more private data points have been made meaning a lot of companies have access to loads of bytes of data on every person. The internet has found itself at a cross-roads, where many people skip the privacy terms and conditions[3]. The interconnected Internet of Things has allowed for a speedy flow of data around to users. When every part of your data is open, how does a person keep their private information from leaking to the public and losing their privacy.

## II. THE WHY & BACKGROUND

When you think about the internet, most people will think of Social Media, Google, Email, or Amazon. All of these services come at a cost. The cost may not be payment in form of

money but in the form of collecting the users data to sell to other companies for who knows what with your information like your email, name, age, etc. There is so much that even one website or app might collect the list is too long to put here. With more people signing on the internet, this has made companies rich with user data that they can use in whatever way they want as long as you signed off the on the privacy terms and conditions. This is the why of this paper to look into the how the internet collects, uses, and distributes your data. Then talks about how you can keep your data from leaving your hands. With privacy a growing concern on most Americans[3], they would like to know what they can do to take their privacy and security back from big companies and keep their information private.

## III. RESEARCH

In my research, I used IEEE Xplore to start off with concrete and reliable data about the Internet of Things and the use of privacy with it. It led me to the this article called, Web of Things: The Security Challenges and Mechanisms[4]. This led to me more finding out information about how the Average American thinks about their privacy on the Internet and if it would

be possible without the collection of their data from big companies or government[3]. Then I thought about the actual amount of user data the Internet Companies hold, which I found my answers in the Our World of Data[2]. These three articles comprised my research, all hold excellent knowledge and understanding of the topic.

#### i. Web of Things: Security Challenges

The authors write about how the start of the Internet of Things (IoT) has changed and evolved into the Web of Things (WoT). As it is the future of integrating smart devices not only to the internet but to the World Web Wide. The WoT is expected to make the accessibility of smart devices easy and promote by combining novel values of web resources to the physical world, such as sensors, appliances, and smart devices. As the connectiveness and use of the WoT grows, the authors have identified key issues with WoT Security, used threat analysis and attack modelling methods, and provided necessary insight into how security can be improved by certain methods. A couple of the Security challenges in WoT include unauthorized access to WoT networks, eavesdropping, Denial of Service Attack, Tempering Attack, and Impersonating. Two that I found very interesting were Eavesdropping, where an attacker tries to steal information that smartphones, tablets, computers, or other devices transmit over the network and Tempering Attacks, is mostly a man in the middle attack, fetching data over the internet and intercepting it between the client and server.

#### ii. Americans and Privacy

The Pew Research Group, a well known and respected research organization, released a report on Americans and how they feel about their privacy and data on the internet. The report starts off with the feeling from a majority of Americans believing that their online and offline activities are being tracked by companies and governments. A metric they talk

about is how "Roughly six-in-ten Americans believe it is not possible to go through daily life without having their data collected", as a regular person can not go on the internet or the web without them knowing that they are being tracked by the government or private companies. Also many Americans feel that they do not have any control over what data is collected about them by companies and the government. The survey goes into a lot more detail about what personal data should be used to help improve schools or assess potential terrorist threats. As Americans question which and where their data should be used, the Pew group suggests that they are open to the idea of using it for potential terrorist threats but not for smart speaker makers sharing their audio recordings with police. There are certain lines that the people will seem to not want to cross.

#### iii. Internet - Our World in Data

The Our World in Data Organization, has collected a lot of data on many things about the internet and people using the internet since the inception of it. It starts off talking about the total number of people and percentages of people in each country who used internet in the last 3 months. As of 2016, their data shows that there are 3.5 billion people who have used the internet which would be just under half the total number of humans on earth. The top 3 countries with the most internet users, include Iceland, Luxembourg, and Norway/Denmark. It goes into the Mobile phone use of the world and the rise of social media. In 2019, Facebook passed 2 billion monthly active users which is about 25% of the world is using Facebook monthly. If you break it down by age groups, young people (18 to 24 years old) are using apps like Snapchat, Twitter, and Instagram more than elder people (65+ years old).

### IV. MY FINDINGS

During the research, I thought a lot about how the average person is using the internet at least once a day in America. How distrustful they

feel about how governments and companies about collecting their data. The goal is to turn the tables of the average internet user's data back into their own hands. As more and more users come online and search, make accounts, and connect with others online; the more data each company has on that person. Which should be limited by how much data and what data should be collected by companies and governments. There are ways to go around this problem, including government regulations and people voicing their opinions. One way is strict, government regulations, and one loose, people's opinions. With government regulations, it is harder to get them passed through and made into real laws for companies to follow. While people voicing their opinions is easier for everyday users to get into and work on as they can organize and demand things from company and the People's opinion is hard for a company to ignore forever.

## V. FUTURE WORK

In conclusion, the interconnectedness of the world as it is today has brought many achievement and accelerations toward every field and job around the globe. But this achievement has come at a cost that people are now waking up to and now not wanting. That cost being their loss of privacy in their lives. These papers offer some insight to the average person that is worried about their data use. As the future holds two possibilities, one with a person's privacy and security of that privacy; or one where the average person has no control or little control over their data and information out on the internet. When the future comes, I hope we are in a world where I do not have to worry about my data being leaked to the internet or being sold off to another company that I do not know about.

## REFERENCES

- [1] Bill Mongan. *CS474: Human Computer Interaction: Research Report*. URL: <https://www.billmongan.com/Ursinus-CS474-Spring2022/Projects/Report>. (accessed: 04.05.2022).
- [2] Hannah Ritchie Max Roser and Esteban Ortiz-Ospina. "Internet". In: *Our World in Data* (2015). <https://ourworldindata.org/internet>.
- [3] Brooke Auxier et al. *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*. Aug. 2020. URL: <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>.
- [4] Ruhma Sardar and Tayyaba Anees. "Web of Things: Security Challenges and Mechanisms". In: *IEEE Access* 9 (2021), pp. 31695–31711. DOI: 10.1109/ACCESS.2021.3057655.