Protecting Oneself in a Digital World

by

Christina A Peralta

A Thesis Presented in Partial Fulfillment
of the Requirements for the Degree
Master of Science

Approved November 2023 by the
Graduate Supervisory Committee:

Scott Scheall, Co-Chair
Keith Hollinger, Co-Chair
Nicholas Alozie

ARIZONA STATE UNIVERSITY

December 2023

ABSTRACT

Due to the internet being in its infancy, there is no consensus regarding policy approaches that various countries have taken. These policies range from strict government control to liberal access to the internet which makes protecting individual private data difficult. There are too many loopholes and various forms of policy on how to approach protecting data. There must be effort by both the individual, government, and private entities by using theoretical mixed methods to approach protecting oneself properly online.

ACKNOWLEDGMENTS

I would like to acknowledge my committee co-chairs, Dr. Scott Scheall, Dr. Hollinger, and Dr. Nicholas Alozie. Thank you, Dr. Alozie, for your guidance and thank you Dr. Hollinger, for helping me out in finding information for my topic easily. Dr. Scott Scheall, thank you for your much needed assistance in helping me complete this thesis. Your support and engagement helped me to move forward and continue writing.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

Unlike physical forms of communication, online privacy and security are difficult to govern. The U.S. Constitution applies foundational privacy measures that laws use to determine precedence for digital privacy protections. The Supreme Court (U.S) recognized the "right to privacy" in *Griswold v. Connecticut* (1965), derived from penumbras from the First, Third, Fourth, Fifth, and Ninth Amendments combined together allowing for a zone of privacy. The Federal government passed the U.S. Privacy Act of 1974 which established rules and regulations regarding government agency's ability to collect, use and disclose personal information. In 1999, the U.S. government signed the Gram-Leah-Bliley Act (GLBA) that protects consumer privacy which applies to financial institutions that access personal data. Financial institutions must take steps to protect individuals' privacy from information sharing by allowing users to opt-in or opt-out. Financial institutions must follow established guidelines that develop and implement security programs to protect customer data from unauthorized access. The Federal Trade Commission (FTC) is a principal enforcer for these laws within the U.S. and in recent years, has taken enforcement actions against companies that have misled individuals about their data privacy and security. Outside of the FTC, privacy laws within the U.S. vary by state. Globally, different countries have different measures.

Technology is a vital aspect of our lives; nothing remains untouched by it today. Access to the online world where we all leave behind a digital footprint via email, and social media. What individuals browse every second of their lives, leaves traces about who our physical selves are. The information gathered by online sources such as Google,

government entities as well as other consumers are used directly to target individuals by extracting data. While a minor issue at first glance, the data is sensitive information stemming from everyday social life, working life and what people do in their private time. Entities, such as Google, can access things people hear and see to use that information to narrow specifics about a person's personal data. The government can help attempt to bypass several of those privacy issues by lessening data gathering by entities through introducing policies that limit data gathering. However, it also makes it harder for internet users to protect themselves and use online services, like Google because these private tech companies can easily deny access if users do not agree to terms. The means of production are owned by society while individual firms' directions can be decided by those within the workforce. This helps stop the exploitation of workers and users as well as help with spreading wealth within the digital economy. This allows data to become capital which would in theory lead to immense amounts of wealth, as well as reducing citizens' dependency on data-sharing companies.

For the reason stated beforehand, it is unlikely that restrictive internet government policies within the United States will effectively curb website tracking to attempt to protect individual user's data. Companies such as Google 'legally' participate in these practices, non-legal entities often operate outside of national borders, and their activities are difficult to track because they can easily bypass online restrictions. Attempting to add more restrictive policies will limit internet freedom and may also limit the ability of law enforcement agencies to monitor and investigate cyber-criminal activities. Moreover, policies are likely to infringe upon civil liberties and bring forth privacy concerns, which is a potential problem that may result in decreased public trust in government institutions.

Restrictive policies may only serve to exacerbate the issue of website tracking by creating an environment in which forces individuals to turn to illicit sources to access information and online services.

This thesis argues that the burden of protecting oneself in a digital world should fall upon not only the individual but include a more effective approach to addressing web tracking to protect user data by involving the individual, government, and entities such as Google. This would involve collaborative efforts between government agencies, private sector organizations, and the continued development and deployment of advanced cybersecurity technologies and strategies. The governments would introduce policies to give entities the minimum privacy protection standard that entities would follow. The individual would have the ability to opt in or out to those standards when using the internet of things (IOT). The important part would be that this method would allow for some sense of balance between digital self and privacy protections without having strict physical laws applying to the digital world. This approach would ensure that users are able to access information, and services securely and efficiently, while also maintaining their right to privacy and freedom of expression online.

CHAPTER 2

LITERATURE REVIEW

With the rise of technology, there is a strong public interest in protecting online privacy which has made it easier to collect individual's data with and without their consent. Digital privacy brings forth a debate between privacy and freedom and the ethics associated with protecting individual user data (Jasanoff, 2016). Privacy is a civil right afforded to citizens by their governments, not to be confused with human rights which are intrinsic to every human. Therefore, the online world does not accommodate privacy for every individual. Governments may choose the right to privacy as an inappropriate right, while other Governments may see privacy as all-encompassing for their citizens. This creates a privacy spectrum that ranges from extreme policies governing every move made in the digital world, to freedom to roam without Government intervention. There are a number of policies and approaches aimed at protecting online data like Digital Socialism (DS), (Muldoon, 2022), Data-owning-Democracy (DS) (Fischili, 2022) to help empower individual users. However, entities meet these approaches with resistance because of the benefit the collection of individual data holds (Clayton, 2006).

The has been recent consensus in regard to the balance between privacy and security that stands up in today's climate. "Privacy and Freedom" (2005) insists on a balance between competing demands of privacy and disclosure. Alan F. Westin (2005) is the most cited book that highlights privacy issues and the impact of technology on privacy. Westin (2015) explains that individuals are entitled to withhold their personal data and have it used by entities. There should be literacy education among individuals (Clayton, 2006) to help them better understand what is occurring with data and privacy

issues. Individuals should alert companies if they wish to have their data used to target their interests. They realize the issues of protecting data and individual privacy are daunting to where the law cannot handle them alone. Westin (2005) acknowledges that the solution requires a mix of legal, social, and technological solutions. Daniel J. Solove (2023) agrees that rights are an important part of privacy regulation, however, the capabilities of law can only do so much. Laws are supporting actors in bigger architecture and cannot serve as a blanket of protection for individuals. Architecture such as automating (Ta, 2022) to explore theoretical algorithms that compare conformance between privacy, data protection and functionality. Broader infrastructure levels are needed to achieve the goal of protecting individual privacy rights.

The global perspective taken in this thesis aims to show how the digital world goes beyond the United States (U.S.) resulting in policies overlapping with other countries as they towards protecting individual data. These organizations such as the Federal Trade Commission (FTC), ICANN (Jongen, 2022), General Digital Protection Regulation (GDPR) create policies that dictate the minimum standards for protecting individual user data that countries and entities must follow. They play a vital role in data protection and privacy due to their intertwining reach globally and the issues surrounding privacy and protection that countries and entities are partaking in. The study of ICANN (Jongen, 2022) is applicable because it explores how ICANN can create policies aiming to ensure equality within this topic without allowing existing inequalities in the organization to set back progress. The cases from the four countries chosen, China (Zhang, Chong, 2020) (Zhang, Chen, 2020) (Xu, 2019), United Kingdom (U.K.), Ukraine (Sopilko, 2023), United States (U.S.) (Schlesinger, 2022) (Boussios, 2016), explore a

range from extreme government regulations to non-existing government intervention and the in-between. The issue is much a social issue as it is a political issue.

CHAPTER 3

ANALYSIS

Privacy Concerns and Threats

The Great Firewall of China is globally considered the most restrictive location in cyberspace because it is a highly sophisticated internet censorship system implemented by the Chinese government. The firewall blocks access to websites and online services deemed politically or morally unacceptable or threatening to the government's authority. While in China the government focuses on monitoring cyber traffic coming in and out while regulating it as much as possible, Ukraine focuses on ensuring that access to cyberspace is free and as open as possible that are focused on ensuring human rights and freedoms, social, political, and economic development, not hindered by strict laws. This method of cyber governance is an attempt to balance the rights of the citizens, government, and rule of law, with an emphasis on sovereignty. The United Kingdom is now in early stages creating a neo-regulatory regime where top regulators will have access and control of statutory powers. There is a critical difference between the notion of freedom of information, privacy, and freedom of the press in the United Kingdom. For example, government censorship of media outlets is standard in the United Kingdom.

DOD (Muldoon, 2022) addresses an issue with allowing for more open source and collective commons can enable more privacy concerns and misinformation to be spread. This method allows for self-governance, and its conception is essential rather than auxiliary to the socialist understanding, because digital socialists allow for the creation of organizations to play an important role in democratic governance by providing equal

access to the digital world across economic, political, and social structures. This raises concerns about ethical and legal aspects of data collection and privacy.

User Behavior and Awareness

There are various ways to trace individuals that often seem and are intrusive available on the internet. Big data, as Jasanoff (2016) calls it, has allowed cyberspace to become a business type area, with the ability to gather information from the many individuals accessing it. Information that is gathered tends to show accurate profiles of a person's identity, appearance as well as their own thoughts. Information can be obtained easily which raises privacy concerns regarding how individuals place data about themselves onto the World Wide Web. The number of devices, such as computers and phones we use are connected on a larger level making anything traceable online. The internet of things (IOT) research also suggests significant threats to privacy by having so many household devices connected to the internet and sometimes reporting data back to the manufacturer. This data within the internet is long lasting and withstands the test of time. This often leads to online information about individuals difficult to remove, compared to removing issues regarding the physical (Jasanoff, 2016). Those three points Jasanoff makes regarding the intricacies of data collection shows how the usage of the internet presents issues for ethics and laws because they easily violate individual rights and begin to display the distinction between our digital and physical selves.

In the beginning of the creation of cyberspace, it allowed for freedom without constraints without any virtual costs to people who understood how to use it. Cyberspace can be compared to the American wild west era, which allowed industries to pop up and

new rules to emerge as it grew. Commercial and now primary source of news and information for much of the world that is disconnected from the grounded physical reality prior to the creation and growth of the internet. Jasanoff's idea regarding an individual's digital self, and how it differs from our physical selves provides insight into understanding the differences between the digital world and physical world and how those differences affect governing. We have "Laws protecting individuals against unwanted intrusions…" that are protected by the "Fourth Amendment's guarantee of the right of the people to be secure in their persons, houses, papers, and effects'," (Jasanoff, 2016). In the physical world, individuals have the right to control their bodies, their own images including an individual's personal signature because it is a part of an individual's physical personal hood. Those protections also extend to components of the physical world such as houses, rooms, anywhere where people do have a right to spatial privacy, autonomy, bodily integrity and henceforth (Jasanoff, 2016). Jasanoff argues that mapping these physical and virtual representations of one's inviolable self is enough to carry over and protect the digital self as well. At first glance, extending the Fourth Amendment beyond the physical world and into the digital world would seem to be a simple policy adjustment. However, this is not the case, because the digital world has become a market for data collection where protection of the digital self's is more difficult compared to our physical identities. An individuals' digital self is defined by all the interactions they have made and will continue to make in the digital world. This digital self enables additional collection by entities in the digital world. People cannot engage with the digital world without being exposed to various forms of data collection. Your digital self is made up data collected by search engines, note that we have this information collected when we

swipe credit cards and sign up for shopping deals with physical world entities, accessing online stores, email, social media, and any type of service where a provider requires information and email regarding an individual. This data is collected in both worlds to build a digital identity. The difference between the two is that when you die in the physical world, your "body dies and memory disintegrates, but [your] digital data can live on indefinitely," (Jasanoff, 2016). The digital self also creates a higher risk of a breach than your physical self. This risk could extend beyond your life to your descendants in the future.

Regulations and Policies

Organizations such as ICANN, GDPR, FTC engage with competition and consumer protections agencies in other countries to promote safer data and privacy protections. The United Nations (UN) General Assembly Third Committee adopted a resolution A/HRC/48/31 recognizing the importance of respecting international commitments to the right to privacy in the digital age.

The General Data Protection Regulation (GDPR) came into effect in 2018 and applies to all organizations globally that have access to EU citizens data. The GDPR sets strict standards that service providers must follow to ensure transparent and secure handling of personal data. Heavy fines are provided to violators who ignore the GDPR provisions by appointing a data protection officer to oversee compliance. The GDPR's range applies beyond U.S. borders which makes it a far-reaching data protection agency.

The United Kingdom emphasizes governance within a legal framework that closely controls cyberspace access. "The United States proposes a principle that on the

one hand adopts an attitude of… compromise... [and] free flow… of [data]" (Zhang, 2020). Then on the other hand, the United States tends to "underscore the importance of government standards… [in] security environments" (Zhang, 2023). Ukraine proposes sovereignty regarding the digital world access that does not infringe on the human rights of people, while China prefers to not display free and open access to the digital world that is entirely controlled by their government. Zhang's (2023) discusses the concept of "Internet Governance" that covers both software and hardware management. This coordination between software and hardware management allows for communication and government coordination that involve both internal and external stakeholders. Is facilitated by democratic participation and autonomous management that is not imposed by a political authority. This allows the independent stakeholders to cooperate under the supervision of an autonomous management agent. Stakeholders would need to relinquish their control over autonomous management agencies like, Internet Assigned Numbers Authority (IANA) to develop "Internet Governance" in a systematic integrated system. Each country has their own propositions that are based on the international rules.

The United Kingdom during the 23rd G8 summit proposed topics and discussions based around their own interests, China wanted to establish new international organizations within the already pre-existing United Nations framework, which would help speed up legislations (Zhang, 2020). The United States proposed and passed the National Cyber Strategy which sets core principles for cyberspace. Overall, there seems to be competition of power concerning state governments and we can see that there is a divide and tradeoffs between "Internet Principles of Freedom" and "Internet Sovereignty" which demonstrate that the supervision of rules requires cooperation between "non-

conventional multinational institutions that shall involve multinational corporations, non-government organizations government agencies and individuals" (Zhang, 2020).

The U.S. Supreme Court decided on June 22, 2018, in the case of *Carpenter v. United States*, that the Government needs a warrant to access a person's cell phone location history, in a 5 to 4 ruling. Obtaining such information falls under the protections of the Fourth Amendment which requires a warrant based on probable cause from a judge. The ruling from the U.S. Supreme Court was based on the Fourth Amendment that protects not only property interested but the expectation of privacy. *Katz v. United States,* 389 U.S. 347, 351, allows an individual to seek to preserve privacy as long as the expectation of privacy is reasonable. Intrusion into that sphere of privacy requires an official warrant to search under probable cause in *Smith v. Maryland*, 442, U.S.735, 740. The analysis of reasonable search and cause was based on the ruling for unreasonable search and seizures when the Fourth Amendment was adopted in *Carroll v. United States, 267 U.S. 132, 149.* The Fourth amendment allows foundational understanding for implementing ruling for modern world surveillance tools in *Kyllo v. United States,* 533 U.S. 27. Information gathered from third-party sources regarding personal location was addressed in *United States v. Jones,* 565 U.S. 400 highlighted privacy concerns with location with devices such as GPS. In *United States v.* Miller, 425 U.S. 435 disallowed expectations of privacy with bank held records. *Smith,* 442, U.S. 735 disallowed expectations of privacy in cellphone records conveyed to telephone companies. Individuals have an expectation of privacy within the United States and believe tracking an individual's movement by cell phone records are viewed as one of the privacies of life. Cell phone records pose data privacy risks because they allow for nearly perfect tracking

of movement of an individual. These privacies extend so far, cell phone records are considered business records, therefore, third party records. Reasonable searches are allowed to seize and gather this data, but only with an official warrant, unless exigent circumstances arise, where a warrantless search will be permitted.

In *Twitter, INC v. Taamneh et al,* May 18, 2023, the U.S. Supreme Court ruled unanimously that hosting, displaying, and recommending videos is not aiding and abetting terrorism. This ruling allows social media platforms to not be held accountable because the platforms are open to all users. The plaintiffs alleged that these companies aided and abetted ISIS in its terrorist attack on the Reina nightclub under the Justice Against Sponsors of Terrorism Act (JASTA) that imposes secondary liability to those who knowingly aids terrorists. Aids and abets was a common law term defined in *Sekhar v. United States,* 570 U.S.729, 733. Congress also added additional context for JASTA in *Halberstam v. Welch,* 705 F. 2d 472, for legal liability and conspiracy to aid and abet based on three main elements. (1) Must be a wrongful act that caused injury by the person who the defendant aided. (2) The defendant must knowingly be aware of the illegal activity. (3) Defendant must have knowingly and assisted in the illegal activity, noted under *Welch*. The Supreme Court goes on to describe six key factors that help determine whether the assistance was substantial enough. The ruling of *Twitter, INC v. Taamneh et al. (2023)* sets the precedent that companies cannot be held responsible for free speech and shared activities on the internet, if shown on their platform. Individuals from around the world sign up for these platforms and upload any content. The amount of data location on these platforms is astounding, thus organizing this information would be

nearly impossible. Context such as the ISIS terrorist attack showed up because of algorithms of individuals and can continuously show even if removed.

The United States Supreme Court case, *Gonzales v Google LLC*, in 2015, ISIS unleashed coordinated terrorist attacks across Paris in 2015. One of the victims was Gonzales, 23, a U.S. citizen, whose family sued Google under the 18 U.S.C. 2333(a), (d)(2), alleging that Google was directly and secondarily responsible for the attack. They argued that platforms such as Google, gained revenue from the sharing of ISIS related advertisements. The Ninth District used the case *Twitter, Inc. v. Taamneh,* U.S. (2023) to affirm the consolidated opinion of *Gonzales v. Google LLC (2023).* The Supreme Court barred the plaintiffs from being recognized under Section 230 of the Communications Decency Act of 1996, 110 Stat. 137, 47 U.S.C. §230(c)(1) and therefore refused to recognize their complaint.

"Section 230 of the Communications Decency Act promotes free speech by removing strong incentives for platforms to limit speech online" (Granick, 2023). This allows platforms to not be liable for content posted by individuals but does not free platforms from liability. The U.S. Supreme has denied hearing in cases regarding data and privacy and applied §230 to those cases, as seen in *Gonzales v. Google, LLC (2023)* dismissal. Data and privacy collection in the digital world is not considered private due to third party entities that these platforms and technological devices use to gather information. Yet, individuals are still in a fight with legalities behind current laws being used as a gray area that has not yet been defined. The United States (US) and the U.S. Supreme Court has no official ruling that sets up policies and laws about data and privacy in which the populace can build upon. The relevance of these current Supreme Court

cases show that the law is not yet defined in the United States (US) and still is an ongoing and current issue.

Technological Solutions

One solution for ensuring entities comply with regulations is automation. Those rules are in the early stages, businesses and companies can maintain a steady foundation by using two types of data and protection requirements: policy language and system architecture design. There are three types of conformance relationships coming from 'DataPro Ve: Fully Automated Conformance Verification Between Data Protection Policies and System Architectures' by Vinh Thong Ta and Max Hashem Eiza (2021). Ta's proposed privacy policy comes from the perspective of the data controller that can be equated to a "service provider who stores, uses or transfers personal data" of users, which "covers data protection and privacy requirements" (Ta, 2021). The system architecture is a combination of the three that allows entities to see how a system is created and how entities within it communicate with each other. This allows for smooth automation and can be found in various services, however the automation itself poses high privacy risks. The verification process that comes with privacy and data protection can take the longest amount of time because of the need for the legal policy to be verified through the architecture systems, to ensure all measures are being correctly inputted. The more data there is to verify the longer the architecture needs to take to go through the necessary steps. The verification process developed can be used for already existing systems because it can model and analyze any type of architecture in place (Ta, 2021).

Allowing policies and laws to dictate and automate tasks that would be beneficial for users and tech companies as a means of streamlining data protection and privacy.

There are two types of reform proposals that have been brought up in recent debates that are data owning democracy and digital socialism (Muldoon, 2022) (Fischili, 2022). Data-owning democracy is the extension of democratic principles in the digital world because individuals have ownership and control over their digital identity in the digital world. It allows for widespread distribution of data as capital among citizens, whereas digital socialism allows for open source software and commons-based Production. But its primary goal is equal access to everyone. It raises significant questions about privacy and data ownership, profit sharing of digital proceeds, and facilitates global social movements. The article, "Data-owning democracy or digital socialism" by James Muldoon (2022) argues that digital assets are ever increasing thus becoming an essential part of the global economy (Muldoon, 2022) as they dominate the market. Companies such as Amazon and Google have vast resources that are comparable to some nation-states. The influence they have over the data allows them to exercise disproportional influence over consumer markets, thus sparking outcries for greater government regulation and oversight over these markets. There is a regulatory need to introduce rules that prevent anti-competitive behaviors and allow competition to continue to flourish within the tech sector. Google, Microsoft, Amazon and other large tech firms, out smaller firms, making it difficult for new consumers to enter the market. This issue causes resistance to digital socialism from critics that demand more protection for individuals and small businesses from unfair competition. Those anti-competitive practices expose entities that have control and ownership over digital assets and offer

solutions on how digital technologies can be used to empower citizens and aid them in this power imbalance.

The theoretical political regime inspired by the data-owning democracy literature can be integrated with digital technology that allows for data to flow easily to the consumer while protecting digital privacy. Some regimes combine "municipally-owned digital infrastructure and collective data ownership rights with copies of individual data flows to empower citizens in the digital realm" (Muldoon, 2022). This allows for greater control and leverage over their own data.

Digital socialism requires government regulation of data markets to help promote equal access for all. It is important to note that both methods focus on collective ownership of rights that help redistribute wealth that allows for communities to participate, to achieve political and economic equality. Digital socialism focuses on creating structures that communities, like creative commons and open-source solutions, can actively participate in thus allowing some governance over digital services by adding "more expansive set of participatory rights that would enable democratic collectives to control public services and play an active role in shaping structure and role of [those] institutions" (Muldoon, 2022). Digital socialism allows people to counter power imbalances to provide equal distribution of resources and participation regarding decision making. Digital socialism requires a multi stakeholder governance that allows participation in how the internet will be governed. Most platforms being used today by millions of users are already forwarding information to data collection companies. However, those companies that would require a multi-stakeholder role are in the majority and would require reform and restructuring to meet the standards of digital socialism.

Social and Cultural Aspects

Cultural variations in attitudes towards individual data and privacy protections, government intervention vary based on countries (Zhang, Chong, 2020). Countries such as China would lean towards more strict regulations where the government had full control to distribute resources to their civilians. Their socialism ensures that no corporation becomes stronger than the government that would create situations that exist in the United States. In the United States there are entities, such as Google, who have more control over the internet of things (IOT). Ukraine's extreme liberal views allows their internet of things (IOT) to be accessible to different actors. Ukraine values freedom and individual expression among their citizens. The United Kingdom (UK) does not have a free press, and privacy rights in the United Kingdom are not protected by a document like the Bill of Rights in the United States. This allows the government to control digital data, however, not to the extreme that China does. The United States (US) government does not control the internet of things (IOT) which allows non-government organizations to capitalize it. Corporations are considered their own entities and are afforded the same rights as the individuals under the constitution. This allows for open-source connections but not as open as Ukraine's government allows its citizens.

Ethical Considerations

To reach another person on the internet, it requires using an IP address that has names and numbers associated with your address that is unique from others. ICANN helps coordinate all information into one globalized internet process. ICANN was founded in 1988 out of U.S. Government commitment based in the U.S. ICANN

separated itself from the U.S. government to ensure global internet users have a say in decisions affecting its management. ICANN's key priority is maintaining a collaborative platform based around data and privacy protection initiatives dedicated to keeping the internet secure and helps promote competition and policy development related to cyberspace. They employ transparent policy development with the help of expert advice and collaboration with entities affected by those policies through a multistakeholder model. ICANN is viewed as a source of global government, however, outcry suggests that these institutions are illegitimate because they incorporate "unfair power asymmetries (Jongen, 2022).

If a global organization that is a vital part of ensuring equality within the IOT is skewed towards certain geopolitical, social, and cultural groups, will ICANN be able to uphold their policy goals? Jongens (2022) survey shows the belief that ICANN steadily remains a key part of global internet governance that can help fix those inequalities stemming from policy creation from those in control of the internet of things (IOT). Four factors highlighted in Jongen's empirical study of ICANN do notice the structural inequalities. People on the subordinate side of ICANN have observed larger inequalities regarding power and influence within ICANN. These inequalities stemming from infrastructure, control, and access to the internet of things (IOT) which shows who benefits and does not from access. Secondly, individuals on the subordinate side, "women and Global South participants- tend to see larger inequalities" (Jongen, 2022). Third, a lack of connection in establishing concerns about these inequalities is apparent because they have not been addressed "long and insistent normative opposition" (Jongen,

2022). Lastly, although ICANN can see these inequalities, ICANN seems unwilling to give them precedence.

The study sampled 467 participants in the global governance at ICANN. "ICANN participants generally perceive… inequalities in the workings of this global governance regime... And hold a consensus about [who are in dominant and subordinate positions]" (Jongen, 2022) that highlight disparities among people who have access to ICANN power that causes structural inequalities. There are notable inequalities based on race/ethnicity, gender, and age as well as geopolitics and language types, which is rather interesting to say because in theory, access to the internet should be a leveling field, yet it is dominated with inequalities. Apparent hierarchies within those structures that allowed for division types to occur and remain in place to maintain the status quo of the dominant class. ICANN has not shown effort to fix those larger power inequalities. Jongens (2022) analysis reveals how participants in the study regard inequalities and how they relate to ICANN's global regulatory arrangements.

The analysis describes the inequalities from 467 global governance participants who were in subordinate positions within ICANN. Participants who have "advanced English skills (dominant group) [found that those] with weak English skills [lesser]" (Jongen, 2022) and grouped separately from the insubordinate group. Weaker English speakers hesitate to join discussions, reducing their chances of climbing the structural ladder, which allowed more dominant fluent English speakers to play down the concerns of the weaker English speakers' inequalities. When gender was viewed, Jongen (2022) saw significant differences in perspectives in ICANN's more technical background and business-related fields where women are less prominent within.

When age was viewed, younger generations viewed a divide with power within ICANN, an issue compared to where participants aged forty and older did not (Jongen, 2022). An examination done between the inequalities within ICANN and legitimacy beliefs towards the global governance institution were questioned. Participants were asked if the structural inequalities with those participating with the regime were subject to disparities. The findings show that structurally subordinated circles generally face more exposure to inequalities while structurally dominant circles have access to more resources and political participation (Jongen, 2022). These inequalities are major issues in modern politics. Overall, there was a lack of theoretical association between the dominant and subordinate groups that could be deemed significant, despite the previous two studies showing great perceptions of inequalities between the two groups. "Participants [gave] less priority to inequality relative to other values when they [accessed] institutional aspects of the regime" (Jongen, 2022), showing that ICANN governance is focused on prioritizing technology over equality. The inequalities within ICANN's global governance do not extend into their global policy development.

Education and Literacy

Finally, we reach ways that individual users can in fact use to protect themselves from data and privacy concerns including, how users can learn about and practice them. This brings into question whether if users can become responsible for their data privacy and protection, would people be literate enough to understand how to do so? Online companies tend to make privacy settings more complicated to opt out than to opt in. There are many disparities between what websites offer in terms of data protection and

privacy compared to how individuals can take responsibility into their own hands. These disparities range from websites offering adequate privacy protection, addressing the opt-in and opt-out feature correctly and whether they are by passing legal legislation to get around having to comply with data protection.

Disparities, such as offering adequate opt-in and opt-out features, help shed light on ineffective practices that ultimately do support individual users using privacy-enhancing technologies (PET) themselves (Clayton, 2006). Many websites ask users to accept or decline cookies on their websites, in theory they are supposed to alert the users of the usage of cookies and tracking practices. Cookies are "information saved by your browser when you visit a website," (Federal Trade Commission, 2023). There have been worries regarding the true effectiveness of cookies because acceptance of said cookie does not mean respect of the users' choice, even more so if the user chooses to decline the cookie. While websites may give the option of accepting or rejecting cookies, the cookies may not have been implemented correctly, or deny users access to websites if rejected. There is a lack of enforcement when monitoring online websites due to the vast majority of services available that would need to be checked over. In the EU, half of website cookie usages have in fact violated the purpose (Mehrnezhad, 2021) of what cookies are initially used for by installing cookies that track and profile individuals before they even accept or decline the cookie. A third of the top websites within the UK meet actual GDPR requirements because they contain dark patterns and the "overall lack usable mechanisms for users" to "[accept] or deny the processing of personal data" (Mehrnezhad, 2021). Many people tend to rely on websites and data-sharing companies

to manage and protect their user data, instead there is the realization that online browsing is not as safe.

However, there are ways that users can take responsibility within their own hands. Individual users can protect themselves by foremost, rejecting cookie notices and using built-in browser options, browser blocking extensions as well as other various PETs. PETs cover a third of data protection and privacy technologies (Clayton, 2006) and using other browsers and search engines, which follow GDPR standards can help users remain more in control by helping with ad-blocking and tracking, etc. Privacy concerns and data protection is bar for the biggest concerns EU and UK citizens have (Mehrnezhad, 2021), therefore, if individual users want more control over their own data, they should consider looking into methods of protection. However, websites tend to make that portion difficult because opting-out is not always as cut and dry as it seems because it limits the functionality of the website. Some websites that will not have cookie options at all. Some may even present cookie notices with no option to opt-out and only opt-in. There are also some websites that have multiple options such as customizable information settings and options, however, they will focus only on opting in. The difficulty with opting out is a form of noncompliance based on the minimum of GDPR standards. Due to the fact that a third of websites do not comply or barely comply with GDPR standards, understanding and implementing PET requirements become even more important privacy enhancing options for users in the digital world (Clayton, 2006). Users can adjust their browser settings to prevent data tracking and delete cookies manually. These PET options are included in "Internet explorer, Firefox, Chrome, Safari on PC and mobile devices," (Mehrnezhad, 2021). The issue with this is that according to the GDPR, manually

adjusting these settings is considered a form of non-compliance because the individual is not supposed to change these settings, but instead rely on data sharing companies to do the data privacy and protection methods. “Around one third of websites [advises] users to change privacy [settings]” (Mehrnezhad, 2021) through website dashboards, but now many will offer this as an option, or ask users to delete or deactivate their accounts to control their privacy (Mehrnezhad, 2021). There are options to add additional browser add-ons to help with privacy enhancing extensions as well as personal mobile and app settings where users can opt-out of interest-based advertisements from these websites and companies.

CHAPTER 4

DISCUSSION

There is no single solution that will effectively protect the digital self by incorporating laws designed to protect the physical self that will be an overlapping solution because the digital world is still in its infancy. Countries also have their own policies that they adhere to for cultural and political reasons. The three points Jasanoff (2016) makes regarding the intricacies of data collection shows how usage of the internet presents issues for ethics and laws because they easily violate individual rights, while highlighting the distinction between our digital and physical selves. An individuals' digital self will persist long after the physical self. Rules applied to the physical self cannot apply equally to the digital self because enforcement of the digital world and physical self-differ. Technology and data sharing do not follow the same ethics or morality of individuals. Data owning democracy (DOD) (Fischili, 2022) (Muldoon, 2022) allows individuals to enjoy the political and economic standing that enables them to actively participate in the creation and usage of data. Allowing individuals to control their own data by making it a 'new' good they possess and do with as they please. It should do so by not replacing existing data protection regulations, instead allowing them to work side by side. Digital Socialism (DS) (Muldoon, 2022) in theory should allow balance between citizens and already existing digital companies in power by allowing political equality between institutions and citizens. Individual empowerment by allowing for collective self-determination and democratic participation.

Ideally, using reforms such as DOD and DS to restructure and help individuals adapt to digital protections with the help as a collective seems to present itself as a

solution. DOD and DS would allow for the protection of civil and political rights by using political institutions in the background to allow citizens to participate. Citizens as a collective would be allowed to act with freedom and equality. Using data owning democracy (DOD), the citizens collectively own the data and choose how they are used through democratic means. This helps prevent the hoarding of data online by a few and leaving the citizens at their mercy. With digital Socialism, this would allow the means of production, cyberspace, and data collection, to be controlled by individuals only, allowing control distribution to be broadly spread in mainly worker-owned firms. Many tech firms pay employees in stocks, so they are partially worker owned. As opposed to centralized to one individual, entity, or corporation, thus allowing political power and economics to be regulated through democratic elections. These ways of governing out control both allow for easier access to managing our digital selves and protecting individuals from being data mined by companies. Instead of letting the individual worry about protecting their digital self, these safety procedures are focusing on the collective society to help protect individuals as a group. The collective would be using resources already available and simply reforming the infrastructure to spread it out, therefore less burden on the individual which gets more complicated when people must manage the digital world by themselves.

One should acknowledge the overlap between digital socialism and data-owning democracy because both theories aim to further empower the citizens through means of ownership and control. They both view digital data as the first step to allowing access to a broader range of digital assets. Both counter the power of private ownership by tech companies like Amazon and Google. A second theoretical aspect they share is that “both

seek to institutionalize new participatory structures for citizens to engage in" (Muldoon, 2022). Lastly, they both aim to redistribute the accessible data within the digital economy because both sides acknowledge the control these digital companies hold.

However, reforms targeted at companies alone will not produce the desired results to improve privacy and security concerns in the digital world. Implementing stricter data protection regulations is different from targeting these issues at the level of individual ownership and control. According to Muldoon (2022), the redistribution of power does not fundamentally change the power imbalance because it would just create new winners and losers, regarding access to digital technologies because there is no change in their current rights to a citizens' data and their unilateral ability to control the commercialization of it. Secondly, the data protection laws that seek to regulate how corporations collect and use the data, are more purposeful approaches to curb the most predatory policies and business models, do nothing to increase the citizens economic power or add value to their owned data (Muldoon, 2022). Data-owning democracy, (DOD) (Fischili, 2022) is limited in scope and practicality of the policies that are being proposed. It relies on cooperation between private tech companies and existing public institutions to organize the democratic management of personal data. It does not, however, address the inequalities that are related to the ownership and control of digital services which means there will be hardly an economic impact when it comes to reform. Not only that, but the data itself can also be used as a means of leverage by various digital corporations cooperating to make control, digital services and profit flow their way.

Digital socialism, (DS) involves systems of deliberation that relate to public investments that while does offer greater public control. The bulk of the digital economy will be socially owned which allows the control of digital data within many hands rather than a few, for example, services with Google or Amazon would be under the control of a board of people that represent the individuals and not the private tech company. There will still be inequalities within digital socialism, however, they will never in theory reach the current levels we have today. Unfortunately, these approaches to data protection are limited to what they can achieve because there are several limitations to data-owning democracy and digital socialism in which not enough information has been studied further upon because they are merely theories in the end. A huge limitation for this is the fact that there is not enough quantitative data to help back up both DOD and DS (Muldoon, 2022) to fully be supported internationally and domestically. They are both viewed as concepts.

After looking into the two most popular proposed policies, it is time we delved into existing data protection policies and systems that have already been implemented. The already implemented data allows policy makers to begin enacting how the individual can protect themselves without a collective helping guide their hands. The strategies used to improve privacy require individuals to go beyond and deeper into websites and settings. The strategies may make navigating through website pages unreadable, which the average individuals do not possess the capabilities to understand how to do it. The average person will find this difficult because internet literacy is not common. Policy makers should consider whether or not individuals are aware of PETs, and if so, how did they learn about it? Some participants from Mehrnezhad studies have had responses

ranging from the help of IT people, family that had taught each other, as well as doing their own technical searching themselves to better understand how to navigate online browsers. Those who were already interested in IT and tech found it easier to research and learn more about data protection and privacy. The complexity behind regulations and how they are enforced alongside the tools that individuals can use ultimately makes for a messy and complex way to navigate online while attempting to protect ourselves. There are disparities between legal requirements and websites that are supposed to include them to help manage data usage and transferring, and attempting to opt-out and manage these privacy and data concerns by oneself is not as straightforward as it seems for users, only adding further complications.

Restrictive government policy results from China have shown that security risks involve exploiting loopholes that Chinese Citizens must go through to access the internet that is not heavily regulated by their government. China is a prime example of an extreme of government led internet policies being used to the extreme to monitor all cyberspace activities. However, regardless of the many cybersecurity tools developed in place to strictly monitor the digital world, there are still various ways that citizens and people can break past China's firewalls.

The Principles of Development that Ukraine's President has chosen shows that with creating the most open and free, stable, and secure cyberspace area they focused on ensuring human rights and freedoms, social, political, and economic development, would not be hindered by strict laws. This method of cyber governance is an attempt to balance the rights of the citizens, government, and rule of law, with an emphasis on sovereignty.

However, this freedom does come with downsides, because it allows cybercrimes to be committed easily as well, within and against Ukraine.

The United Kingdom (UK) "highlights [the] tensions of approaching platform regulation and the difficulties governments face to support innovation yet ensure safe spaces for users" (Stilinovic, 2022). The United Kingdom is now in early stages creating a neo-regulatory regime where top regulators will have access and control of statutory powers. This is a prime example of what it is like to be in the middle ground regarding access to the digital world, in terms of government power and protecting individual privacy and security in the digital world.

The United States' perspective on cyberspace along with the inability to be transparent with citizens within the nation, shows a lack of accountability which is vital "in gaining the confidence of the public and 'checking' against abuse" (Boussios, 2016) to avoid overstepping boundaries and trampling on individual freedoms.

The ability to access and participate within cyberspace can be impacted by economic and societal inequalities which are not always guaranteed to help with national and international efforts. In 'Who bypasses the Great Firewall in China,' (2020) Chong Zhang discusses the digital where internet access was mostly limited to homes. Cell phone towers did not provide reliable access to the internet, and it was not fast. So only those who could afford a computer and monthly internet access bills could access the internet. It was a function of an evolving technology. The first to enter pay the most, over time the cost of access goes down. The divide separates the haves and have nots in terms of who has access to cyberspace, which compared to the 1990's is far more attainable now with the internet on cell phones made the most significant difference, but

it is far from disappearing. However, the new issue it brings up is who has access to by passing security measures is one of the goals of equality. Like previously shown with China's firewall, when countries have restrictive access to the internet. Access to the internet allows for capital enhancing abilities and "some kind of internet use... are more likely to increase one's life chances" (Zhang Chen, 2020) in terms of education, work, personal life, and political participation. In the research they have conducted it shows that there was a relationship between socio-economic characteristics of citizens within China using the internet to bypass China's firewall. Individuals who bypassed security measures by exploiting loopholes were also "more likely to be young, belong to higher socio-economic, well-educated and urban living areas… especially those focusing on capital enhancing uses of the internet" (Zhang Chen, 2020).

The countries reviewed in this thesis highlight the structural inequalities that have a significant impact on how legitimacy is perceived in beliefs related to global governance regarding privacy and security in the digital world. These inequalities can create a sense of mistrust in the institutions tasked with enforcing cyber laws, especially amongst historically marginalized communities who may feel that the rule of law is not applied equally. This can lead to a lack of legitimacy of global governance structures and an unwillingness to comply with their regulatory frameworks. To combat these issues, laws and institutions are being put in place to make the internet a more multi-stakeholder position, aiming to avoid power being centralized to one government.

Any unequal participation regarding capital enhancing that requires the internet is essential for individuals, and lack of access shows social inequalities further widen the gap of those marginalized communities. For example, higher earning individuals within

China in well developed areas were able to bypass China's firewall and access more diverse resources and information, which disproportionately affects poorer and rural communities within China, placing them at an unfair advantage. The overlapping should help ensure there is more access to cyberspace from poorer communities because infrastructure can be created.

The entirety of protection should not focus on the effort of the individual, but rather, a multi-stakeholder approach that includes the individual. Considering that the world and cyberspace included is globalized, we would have to realize that it would be difficult to ensure that all stakeholders involved would be willing to participate fully because there are many variations from country to country in terms of how they manage their cyber security access. The overlapping of organizations should help promote internalization of cyberspace and internet access while avoiding excluding government agencies completely, allowing for a global stakeholder process. The issue with policy making in this regard is that there is no policy that will fit all online protection needs, nor do I claim that it will all be perfect in the end. But rather a work in progress that needs every entity and individual's collaboration as we take and remove what is needed to encourage the beginning of a cohesive safe online environment.

CHAPTER 5

METHODOLOGY

CASES

China

The Great Firewall of China is globally considered the most restrictive location in cyberspace because it is a highly sophisticated internet censorship system implemented by the Chinese government, which blocks access to websites and online services deemed politically or morally unacceptable or threatening to the government's authority. Dr. Richard Clayton, in his paper, “Ignoring the Great Firewall of China,” (2006) explains how the Chinese Government also monitors online activities and filters content based on keyword searches, by inspecting web (HTTP) traffic, which can trigger alerts to officials if users enter certain monitored keyword; including topics related to democracy, religious freedom, human rights etc. Chinese citizens still find ways to bypass the security system by using Virtual Private Networks (VPNs), which can encrypt online activity and provide a secure connection that cannot be tracked or intercepted by the government. Another method is using proxy servers, which act as intermediaries between a user's computer and the internet, allowing them to access blocked content without being detected. Some internet users in China also use Torrent, a free web browser that can be used to access blocked websites without revealing the user's identity by changing IP addresses continuously (Clayton, 2006).

To highlight how the Chinese firewall blocks connections, Dr. Richard Clayton (2006) conducted experiments in which they “were accessing a website based in China [within the Chinese Firewall] from several machines based in Cambridge and England

[outside of the Chinese Firewall]" (Clayton, 2006). The Chinese Firewall is meant to detect content being filtered that goes back and forth between machines, and in this experiment, they were able to successfully go through The Chinese Firewall via Cambridge, without breaking Chinese law. The next portion of the experiment was adding a keyword that would have been expected to be blocked, in which The Chinese Firewall validated the request three different times to which only a partial information request was sent back, before being blocked. Their firewall does not only inspect the content but has other blocking capabilities as well. When 'bad' connections are made between hosts, all traffic between those areas is completely blocked off for a duration of time. The Chinese Firewall does not focus on resetting and helping the connections get through, instead they focus on blocking them, in time limits ranging from a few minutes to hours, through various other devices that help the firewall and its functionality (Clayton, 2006)). Requests being sent between devices will often be ignored if they do not fit standard TCP/IP address protocol standards used for verification, which is a major loophole within the Chinese Firewall. This allows data to be sent through, instead of being checked and validated, allowing people to bypass the firewall. This issue, while minor at first glance, gives enough time for cyber attackers because it allows an open window "to identify machines used by regional government offices and prevent them from accessing Windows Update… or prevent them from accessing specific UN websites," as well as "prevent[ing] access by Chinese embassies abroad," (Clayton, 2006) from communicating back and forth with China. These small loopholes, even within the most restrictive firewalls out there, make it easier to spot flaws, and allow cyber crimes easier access into the protected cyber spaces. Not all IP addresses get inspected, only

about two thirds of them sent from the study were checked. They were able to reverse engineer the algorithm The Chinese Firewall used to validate and scan incoming IPs and content.

Ukraine

Ukraine displays a complete opposite compared to China where cyber security laws of Ukraine emphasize legal and organizational basis that protect the interests of their citizens, society and of the state. These rights are ensured and based on the "Constitution of Ukraine and the Convention on Cybercrime… in the context of ensuring the constitutional rights of citizens" to ensure "sustainable development of information society and digital communication environment" (Sopiiko, 2023). While in China the government focuses on monitoring cyberspace traffic coming in and out while regulating it as much as possible, Ukraine focuses on ensuring that access to cyberspace is free and as open as possible.

The United Kingdom (UK)

The United Kingdom (UK) has an interventionist approach that allows legislative and administrative measures to take control of cyberspace. By allowing their government control it gives their technology market in cyberspace more reaching power. The UK has increased formalized collaborations of regulators which have engendered emergent designs that constantly reshape the digital landscapes. The collaboration advocates for "whole of government and one stop shop" approach that is intended to facilitate regulatory coordination… and" (Schlesinger, 2022) which allows these regulators to be

more approachable and accessible to businesses and government. This raises concerns regarding effectiveness of this approach because the United Kingdom takes a "soft law" (Schlesinger, 2022) approach while claiming rigorous enforcement. For example, the United Kingdom has previously removed other non-government stakeholders, such as tech companies, from their networks because they posed significant security risks. The success of these regulations in the UK will depend on their ability to effectively demonstrate whether anti-competition agendas would not fight against pro-competition agendas. The consequences of not being able to balance the integration of non-government tech companies could suggest that removing any non-government stakeholders as security risks was initially the correct move. The United Kingdom does not have a free press, and privacy rights in the United Kingdom are not protected by a document like the Bill of Rights in the United States.

The United States (US)

The U.S. Constitution is applied for foundational privacy measures that laws use to determine precedence for digital privacy protections. The Supreme Court (U.S) recognized the "right to privacy" in *Griswold v. Connecticut* (1965), derived from penumbras from the First, Third, Fourth, Fifth and Ninth Amendments combined together allowed for a zone of privacy. The Federal government passed the U.S. Privacy Act of 1974 that established rules and regulations regarding government agency's ability to collect, use and disclose personal information. In 1999, the U.S. government signed the Gramm-Leach-Bliley Act (GLBA) that protects consumer privacy which applies to financial institutions that access personal data. Financial institutions must take steps to

protect individual's privacy from information sharing by allowing users to opt-in or opt-out. Financial institutions must follow established guidelines that develop and implement security programs to protect customer data from unauthorized access. The Federal Trade Commission (FTC) is a principal enforcer for these laws within the U.S. and within recent years, has taken enforcement actions against companies that have misled individuals about their data privacy and security. Outside of the FTC, privacy laws within the U.S. vary by state.

Cybersecurity regulation in the United States tends to be political and contentious. The openness of the internet could allow attacks towards the Nation. The United States focuses on deterring attacks by denying them access to useful information or benefits from attempting to access cyberspace within the nation, yet however, the government refuses to be transparent about its methods regarding cyber security. "The U.S. can only talk in vague generalities about its capabilities" (Boussios, 2016) which makes one believe they are purposefully inflating their capabilities or preventing a researcher in another country from backward engineering it, selling bypasses on the internet in other countries, and create a threat wherein our cybersecurity practices are obsolete. Or perhaps underinflated to make sure adversaries underestimate our capabilities. However, the large defense budget behind cybersecurity also says otherwise. Political leaders themselves are also unwilling to share exactly how the United States's cybersecurity force is run. Which could be because the main actors currently include the Department of Homeland Security, National Security Agency, and the Department of Defense. These actors are a civilian government role, NSA, a military role, and federal role, respectively, which displays how the differences in organization within the United States can make it

difficult to track and include comprehensive oversight among all roles. The coordination of these agencies has been created along with the creation of the DHS. These are highly coordinated agencies focused on protecting our digital world.

CHAPTER 6

CONCLUSION

What may have been viewed as a minor issue is beginning to evolve as technology keeps pace with technological demands but outpaces laws and regulations. This situation allows for loopholes to appear and be exploited as individuals use technology as a part of everyday working and personal life. Everyone has a digital footprint that is left behind and there is no getting rid of it. Likes, interests, needs; information gathered by online sources, such as corporations, government, entities, other consumers, and criminal actors, can be used target individuals for different reasons. This is a form of invasion of privacy because technology cannot be governed in the same way that people can. Not because governing the digital world will not work, rather, the policies cannot be fully enforceable because the behavior of individuals in the digital world cannot be regulated by the same ethics and morality of individual in the physical world. How does oneself protect breeches of online data that individuals as consumers and corporations cannot fully control? What are the various options that have been proposed feasible and morally aligned with protecting our digital selves? Individuals can learn internet literacy from one another. IT knowledgeable people can passed down this information that is self-learned. Individuals have yet to reach a point in our society where internet literacy is a common point of education among. The current infrastructure is not ready to handle individuals handling their data on a massive scale. Partly in due to data-sharing companies that already have accumulated data is available to a select few. Partly because there is lack of internet literacy among the populations. To try and manage all those services would be difficult and pointless because most digital world capabilities

would be controlled by users who do not have the resources to protect themselves against data breaches or attacks, let alone maintaining their own digital selves. Allowing for slow separation and integration of various entities into already existing resources as a collective society rather than only allowing for individual data-sharing companies to have access. The means of protection, data collection and so forth can be controlled by various entities and the individual should in theory allow for fair reallocation of resources and easier integration. The individual will not have to worry about maintaining their own data which may allow for more IT literacy to develop among society, instead of relying on a select few entities to understand how to handle it completely. This route would ensure transparency and trust and possibly introduce digital privacy and security learning into the mix of infrastructure reform and policy creation. Overall, the goal is to create a more equitable and transparent global governance system that ensures the protection of individuals' data and limits the power of any one particular entity in the enforcement of cyber laws.

REFERENCES

Boussios, Emanuel G. “The ‘Right’ to Privacy? - The Debate over the United States Government’s Control over Its Cyberspace.” Athens Journal of Law (online), vol.2, no. 4, 2016, pp. 211–24, https://doi.org/10.30958/ajl.2-4-1.

Carpenter v. United States, 585 U.S. 16 - 402 (2018). https://www.supremecourt.gov/opinions/17pdf/16-402_new_o75q.pdf

Clayton, Richard, Steven J. Murdoch, and Robert NM Watson. "Ignoring the great firewall of China." Privacy Enhancing Technologies: 6th International Workshop, PET 2006, Cambridge, UK, June 28-30, 2006, Revised Selected Papers 6. Springer Berlin Heidelberg, 2006.

Data Protection and Privacy. ICANN. (n.d.). https://www.icann.org/dataprotectionprivacy

Fischili, Roberta, Data-Owning Democracy: Citizen Empowerment through Data Ownership ... 19 July 2022, https://journals.sagepub.com/doi/10.1177/14748851221110316.

Gonzales v. Google, LLC, 598 U.S. 21-1333 (2023). https://www.supremecourt.gov/opinions/22pdf/21-1333_6j7a.pdf

Granick, J. S. (2023, April 14). *Is this the end of the internet as we know it?: ACLU*. American Civil Liberties Union. https://www.aclu.org/news/free-speech/section-230-is-this-the-end-of-the-internet-as-we-know-it

“Internet Cookies.” Federal Trade Commission, 2 Mar. 2023, www.ftc.gov/policynotices/privacy-policy/internet-cookies.

Jasanoff, Sheila. The Ethics of Invention: Technology and the Human Future. 2016.

Jongen, Hortense, and Jan Aart Scholte. "Inequality and legitimacy in global governance: an empirical study." European Journal of International Relations 28.3 (2022):667-695.

Mehrnezhad, Maryam, et al. “How Can and Would People Protect from Online Tracking?” Proceedings on Privacy Enhancing Technologies, 16 Sept. 2021, https://petsymposium.org/popets/2022/popets-2022-0006.php.

Muldoon, James (2022) Data-owning democracy or digital socialism?, Critical Review of International Social and Political Philosophy, DOI:10.1080/13698230.2022.2120737.

Ritchie, J. N. & A., & Jayanti, S. F.-T. and A. (2023, June 16). Federal Trade Commission. https://www.ftc.gov/

Schlesinger, P. (2022). The neo-regulation of Internet platforms in the United Kingdom. Policy & Internet, 14, 47–62. https://doi.org/10.1002/poi3.288

Solove, Daniel J., The Limitations of Privacy Rights (February 1, 2022). 98 Notre Dame Law Review 975 (2023), GWU Legal Studies Research Paper No. 2022-30, GWU Law School Public Law Research Paper No. 2022-30, Available at SSRN: https://ssrn.com/abstract=4024790 or http://dx.doi.org/10.2139/ssrn.4024790

Sopilko, I. M., & Cherevatiuk, V. B. (2022, September). Cyber security and personal rights under the legislation of Ukraine. DOAJ: Journal of International Legal Communication. Retrieved May 3, 2023, from https://jilc.e-science.space/wpcontent/uploads/2022/11/JILC-2022-6-3-018-025-Sopilko.pdf.

Twitter v. Taamneh, 598 U.S. 21-1496 (2023) https://www.supremecourt.gov/opinions/22pdf/21-1496_d18f.pdf

Ta, Vinh Thong, and Max Hashem Eiza. "DataPro Ve: Fully Automated Conformance Verification between Data Protection Policies and System Architectures." Proceedings on Privacy Enhancing Technologies, 16 Sept. 2021, https://petsymposium.org/popets/2022/popets-2022-0028.php.

United Nations. (2021, September 15). *A/HRC/48/31: The right to privacy in the Digital age - report ... - OHCHR*. United Nations Human Rights Office of the High Commission. https://www.ohchr.org/en/documents/thematic-reports/ahrc4831-right-privacy-digital-age-report-united-nations-high

Westin, A. F., & Solove, D. J. (2015). *Privacy and freedom*. Ig Publishing.

Xu Hanming & Zhang Xinping (2019) The Rule of Law Model of Internet Governance*, Social Sciences in China, 40:3, 135-151, DOI:10.1080/02529203.2019.1639960.

Zhang, Chen. “A Comparative Study of the Global Internet Governance System Between China and the United States.” Indian Journal of Science and Technology, vol. 13, no. 23, 2020, pp. 2303–10, https://doi.org/10.17485/IJST/v13i23.774.

Zhang, Chong. "Who bypasses the Great Firewall in China?." First Monday (2020).