Spring 5-19-2023

GDPR, Privacy and Europe's Power Gambit

Daniel Maneloveg
daniel.maneloveg@gmail.com

The GDPR, Privacy and Europe's Power Gambit

In Partial Fulfillment of the Requirements for the Degree

Master's of Art

In

International Studies

By:

Daniel D. Maneloveg

University of San Francisco

Under the guidance and approval of the committee, and approval by all members, this thesis project has been accepted in partial fulfillment of the requirements for the degree.

APPROVED:

_____ _____

Capstone Advisor *Date*

_____ _____

MAIS Director Date

Table of Contents

Acknowledgments

I want to acknowledge everyone who has loved and supported me over the past six years as a USF student. My family, friends, classmates, professors, coaches, teammates, and all the random people I have met on the streets of San Francisco over the years. You have all been a part of the journey and I am forever grateful.

Both the MAIS program and the Politics department at this school have taught me lessons that will remain valuable to me for the rest of my life.

To the diverse and deep relationships that have shaped my world for the better

Thank you

Dedicated to all who know how why or should

Abstract

This paper examines the current state of data privacy laws, with a specific focus on the European Union's General Data Protection Regulation. It begins by defining privacy as a fundamental aspect of the liberal worldview and discussing the history of privacy legislation to show that protecting privacy has long been a commitment of liberal countries.

The paper then discusses how technology has progressed and exposed the inadequacy of previous privacy laws, citing scholarly literature to emphasize the urgent need for updated legislation. It provides an overview of updates made to privacy legislation before the GDPR was passed in 2018, followed by an analysis of the GDPR itself.

The paper concludes that the GDPR has moved the conversation surrounding privacy in the right direction, but it has shortcomings in its crucial components, resulting in vagueness. Therefore, the effectiveness of the law is questioned. Finally, the conclusion is drawn that while the GDPR is a step in the right direction, more study and effort on the part of lawmakers are necessary to effectively protect privacy in the digital age.

Keywords: GDPR, European Union, Privacy, Power, Sovereignty, Public Utility

Introduction

The information age is an era in history defined by its wide scale adoption and development of digital technologies to create, use, and store information. Also known as the digital age or the computer age, beginning in the 20th century with the popularization of personal computers and the internet, the way humans communicate, interact, learn, and work has been transformed. New industries have been born that have transformed the way power relations are understood where access to data and personal information are now legitimate sources of power both economic and political. The shift in the understanding of power has forced a re examination of how nation-states expect to maintain their legitimacy and maintain supremacy of the international order.

The technology developed in the information age caused an explosion in human knowledge in many areas, everything from healthcare to economics, and has created new areas of knowledge such as artificial intelligence and machine learning. Never before has there been such an explosion in new technologies. While the technologies developed in the last half century have undoubtedly contributed to human progress and increased quality of life, there are still concerns. Access to large amounts of personal data of private citizens has given increased power to governments and businesses alike and has eroded public trust in institutions that have long been pillars of society. Ideas like state sovereignty and capitalism, have been the basis on which the international order has founded itself. If we continue to define power as access to information, it is private and non-state, not nation-states or governments, that hold more keys to power

and threaten to undermine the very democratic systems that are foundational to the international order.

Privacy is an idea that had to be redefined in the information age, what was once an unalienable right to be protected at any cost has been eroded due to the pervasiveness of data sharing technology. Privacy was enshrined in the founding documents of institutions such as the United Nations, The European Union, and The United States, and has been understood in many different ways in different places and at different times, but one thing is clear it has always been worth protecting.

The erosion of personal privacy is a defining feature of the information age. It has never been easier for governments and private actors to track the activities of citizens through the internet. Through digital technologies, private capitalist companies hold vast amounts of information on individuals that have given them the ability to change economic and political realities across the globe.

With the definition of power as access to information and with nation-states no longer being the holder but private corporations, and the right to a private life under threat, the question this paper will answer is how nation-states will respond to the power challenge from private corporations who are not beholden to the same institutional checks. Specifically looking towards the policy solutions that have been offered in the European Union that have sought to answer this question.

This paper will focus on how the European Union has attempted to answer those questions. First, the history of privacy laws will be discussed showing the long history of this issue being relevant. Followed by an analysis of how this current moment calls for a new chapter in this history of privacy laws as the technology that surrounds us has

outgrown the previous generation of laws. Moving on to the literature review which will cover from a scholarly perspective why new laws are needed and how lawmakers should go about writing those laws. Finally, this paper will move into the case study section where a deep look will be taken at the GDPR from its formation, the text itself, and a short summary of its success and failures to date.

Before beginning any study, the question of why should be asked. Why is this issue important, why is it worth studying, and fighting for. This paper will address the right to privacy and how it is understood, how it is being threatened, and what will be lost if this right goes away. Privacy is having the choice to decide who has access to ourselves, our bodies, our thoughts, and our relationship with the outside world. In many ways, the right to privacy is the gateway to all other sacred rights; without it, those other rights are at risk of violation.

There are those who say that privacy is dead and that the information revolution has killed it. Mark Zuckerberg once claimed privacy is no longer a “social norm,” but this paper will argue that this can not be true and that it is more important than ever. In the past, when an industry has sought to intrude on a basic human right, there has been a response to protect that right, and this moment calls for the same. In the words of Washington University privacy law professor Neil Richards, “Privacy isn’t dead, but it is up for grabs.”

History of Privacy Laws

Lawmakers from around the globe have been concerned with privacy for generations. We have seen multiple waves of privacy legislation as a response to the state of technology at the time. In addition, governments that claim to champion democracy and capitalism in liberal societies have been mainly concerned about privacy. Here the origins of the right to privacy will be discussed.

Possibly the first modern act aimed at protecting the right to privacy is found in the 1948 Universal Declaration of Human Rights, which in article 12 states, “ No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation.”A relatively basic and broad statement. Created by the United Nations shortly after its founding, it establishes the modern concept of the right to privacy and lays the foundation for future laws. Establishing the right to privacy as a fundamental human rights issue puts pressure on lawmakers to prioritize protecting it from future intrusion.

As the world became more digitized and personal data began being stored on computers, lawmakers understood that updates to their commitment to the right to privacy needed to happen. This is the moment we see a divergence in the understanding of privacy and approaches to protection between Europe and the rest of the world. The first acknowledgment of the need to protect privacy in digital form came in 1970 with the formation of the Younger Committee in the United Kingdom, which was established to study the effect the rise in computers would have on people's privacy. In short, the committee concluded that existing legal measures were inadequate to protect privacy from the new threat of digitization. While the committee's report offered no policy

solution for the threat identified, it began to plant the seed in the public's mind that a new conceptualization of privacy was needed.

It wasn't until the 1980s that global data privacy guidelines were issued. The Organization for Economic Co-operation and Development (OECD), a group of European and other Western nations, came together to write recommendations on Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. This non-binding agreement sought to get ahead of the coming wave of new technologies that allowed instantaneous communication across borders. Here, we begin to see some similarities to current legislation and concerns. The recommendations included ensuring that all data collected is relevant for its intended purpose, individuals having the right to know who is collecting their data and for what reason, granting individuals access to the data collected on them, and the right to be forgotten is still relevant today. While only guidelines and not hard law, the OECD is still an influential organization of some of the world's wealthiest and most influential nations; the standard was established on how the democratic, capitalist world would grapple with the growth of new transnational technologies.

Fast forward to 1995 to find the passage of the first truly legally binding legislation concerning data privacy that seeks to regulate the activities of private companies. The European Union's data protection directive (DPD). In the years leading up to the passage of the DPD, many European countries had passed their laws regulating the processing of personal data, and the EU sought to harmonize the laws within the Union. The defining new feature that separated the DPD from previous legislation was that it created rules for data of EU citizens processed outside EU

borders. In addition, it listed countries EU lawmakers deemed safe for data processing to occur. 1995 was indeed the dawn of the internet age, but still long before nearly the whole world had instantaneous access.

Around the same time, in 1996, the United States passed its law seeking to project its values on forming the digital sphere. The Telecommunications Act, signed into law by President Bill Clinton, essentially eliminated all regulations for corporations operating on the internet and allowed anyone to enter the communications business online. An explosion in the number of companies that could operate on the internet occurred. This act can take credit for changing the way we communicate with each other and can instantaneously connect with people from all over the world. However, the deregulation of the internet has led to many pros and cons. Large communication companies merged without antitrust violations; for example, Time Warner and Viacom merged and shored up a significant portion of telecom infrastructure in the country. Internet Service providers were now in complete control of how they operated, what they allowed on the platforms they hosted, and allowed companies to conduct business with little oversight. Many companies flourished under this free environment, creating new and innovative products for consumers, allowing companies whose primary focus was personal data processing to develop uninterrupted. As the internet spread globally and the pace of technological innovation sped up, these companies could hone their practice on privacy invasion of internet users freely. The law has shaped the internet as we know it as an open forum free from the arms of regulation and open to all voices and businesses. With American companies free to operate unregulated, it gives merit to the concerns voiced by European leaders that foreign entities are overtaking them. To

understand how this environment allowed for the advent of new data extracting practices, there must be a closer examination of that timeline of advancement in technology between the passage of both the 1995 EU data protection directive and the 1996 US telecommunications act.

An analysis of technology progression

The technology that shapes our world has fundamentally changed since the 90s when the day's legislation was designed to govern what was current. It is only logical that technological progress is followed by improvement in government regulation strategy. How technology has changed and challenges, the previous generation of laws is critical in understanding if this current generation of policy is in line with the state of technology and uses sufficient mechanisms to enforce the law.

This section will provide a brief history of technological innovation since the passage of the 1995 EU data directive and the 1996 telecommunications act, as well as an analysis of the discourse surrounding what ways advancements challenged regulatory mechanisms. The works of Halavais, McCarthy, Moy, Vander Maelen, and others will be part of the analysis. Finally, this section will paint a clear picture of why the European Union felt it was necessary to pass such a sweeping piece of legislation like the GDPR and provide a framework for evaluating its effectiveness.

The defining feature of the technological progress of the last 25 years is the rise in the globalization of culture and the ease of ubiquitous and instantaneous communication across the globe with little respect for traditional national borders.

American social data scholar Alexander Halavais writes on how the decentralized nature of the internet has allowed creators and businesses alike to draw links to other

parts of the web as they like, regardless of where they are located. The best version of the web is interconnected, where people can communicate and freely exchange ideas without preference for nationality. This is what lawmakers imagined when passing the laws of the mid-1990s, hoping that it would foster innovation and create a truly globalized market. Halavais questions if the dream of an unregulated web came true and if it allowed for the democratization of culture as hoped for. The opposite was found; 70% of global internet traffic flows through the United States. This gives American companies a considerable advantage in conducting business online. What was designed to bring more voices worldwide has led to a concentration of power and information within one nation. This trend alarmed lawmakers and was a key motivating factor in the data laws that have been passed. Now, as the primary goal of technology companies has become the collection and processing of personal data, this trend will lead to the majority of data information of individuals worldwide being concentrated in the United States in the hands of private entities.

Communications scholar Mark MacCarthy provides us with the idea of “data power” when large companies have collected access to a large amount of personal data that translates into economic strength. Companies acquire data power by simply tracking their user's activities on their platforms; over time, platforms with a large user base can collect a massive amount of personal data, frequently sensitive information.

Companies like Alphabet, Meta, Apple, Amazon, and Microsoft are the most prominent personal data collectors. Alphabet and Amazon also host and store the data of many small businesses through cloud computing, which is nothing more than a digital database of information stored on a private server. It is impossible to avoid interacting

with large tech companies that collect large amounts of personal data, even when not directly using their services, from how we communicate with each other to the many jobs that require being online. Expecting anyone to live an everyday or comfortable life without interacting with these companies is unrealistic. It then raises the question if these companies are such an integral part of modern society and collect such intimate information, what level of responsibility should they be held to? Other industries that hold crucial positions in societal infrastructure, such as public utilities, are held to high standards and are subject to strict regulations. Still, large tech companies have so far escaped the same classification. In her testimony in front of the United States Senate Committee on Science and Technology, professor Laura Moy called information sharing services provided by tech companies “essential and necessary for participating in modern society”.

There is a precedent for bringing private companies that provide essential services under public control. For example, water and electric services are provided by private companies but classified as public goods and something all people need to survive. In the past, railroad, electric, and telephone companies have all been regulated through antitrust laws. The antitrust laws applied to electric and telephone companies aimed to break up monopolies in the industry, promote competition and limit exploitation. Looking towards the information technology industry, specific characteristics of monopolies are seen. Alphabet, for example, is the site for 93% of all web searches globally, Meta has acquired other social networking companies such as Instagram and WhatsApp, two of the most popular social networking platforms around

the world. These companies have a monopoly on collecting their product, which is individual personal data, and use that to create profit.

The other characteristic of a monopoly that needs to be analyzed is that the market structure leaves the consumer unable to leave or seek services from another company. It has already been established that social networking and the internet are essential for participating in modern society. However, there are alternatives to Alphabet and Meta; how can regulators consider these companies a monopoly when an alternative is just a click away? As established, Alphabet hosts a vast majority of web searches around the globe; over 70% of adults are on Meta owned platforms, so to connect with peers, it is challenging to avoid Meta.

Even with it being established that a few large companies control such a large amount of the tech industry, the question remains whether their products and services are genuinely public goods in the same way electric and water are classified. First, it must be established what exactly is the product of Alphabet or Meta. Continuing to use the water and electricity comparison, it is easy to identify their products, but there is a cost to the consumer in using those products. Social media and technology companies are often free. On the surface, the product or service people receive is the information from an Alphabet search or the connection they made on a social networking site. However, are those public goods? Probably not. However, if we define the product of big tech companies as the data they collect, which they then package and sell to advertisers as the product, the public utility factor becomes clearer. At the end of the day, the data collected comes from the public, should it not be controlled by the public. Currently, tech companies have one motive in dealing with the personal data collected,

to turn it into profit, and do not consider the consumer's rights. Regulations have forced water and electric companies to prioritize providing their services to the public as efficiently as possible, even if it means sacrificing profit due to the importance of their products. Can lawmakers create a regulatory framework that ensures that tech companies act responsibly with the data they collect?

Accepting that the services provided by Alphabet, Amazon, Meta, Apple, and Microsoft are essential to a person's ability to live in modern society comfortably, it is logical that these companies should have an enhanced responsibility to their customers and be transparent in how they are handling the sensitive personal information they collect. As mentioned above, companies that provide electricity, fuel, and water are subject to strict government controls. Therefore, it is not unreasonable to claim that technology companies should be placed in the same category as utility companies and labeled as public goods. The problem with this idea is that the technology companies have proven difficult to regulate due to the nature of their products.

In the past, lawmakers have not shied away from enforcing antitrust laws on emerging technology sectors. As early as 1890, regulators have been working towards curbing the monopoly power of large private industries. The United States passed the Sherman Act, which called for free competition among those engaged in commerce and prohibited anti-competitive agreements. In Europe, the 1957 Treaty of Paris was signed with similar aims. An excellent example of a company that was brought under control through antitrust legislation is AT&T, which was an innovator in telephone technology in the early 20th century. Free market conditions allowed AT&T to acquire many of its competitors and gobble up the rights to much of the infrastructure telephone use.

Between 1921 and 1934, AT&T acquired 271 of its competitors, and the attitude of regulators at the time was that it was a natural part of the free market. By the end of world war two, AT&T was by far the dominant player in the telecommunications industry and showed all the characteristics of a monopoly. However, attitudes by this time had changed on the permissiveness of allowing a monopoly in such an essential industry. A 1939 congressional report stated, “The importance of the (telephone) industry calls for actual and not nominal regulation. The telephone business is a monopoly – it is supposed to be regulated. Thus far, regulation, particularly by the Federal Government, has been nominal largely because Congress has not made appropriations sufficient to enable the Interstate Commerce Commission to give effect to existing statutes.”. This report kicked off a multi-decade pursuit of breaking up the monopoly that AT&T had built. After multiple antitrust lawsuits, it was not until 1982 that the U.S. Justice Department could enforce a break up of AT&T into smaller regional operators.

AT&T’s rise to a monopoly parallels the stories of modern technology companies dominating their industry. The lesson learned is that the government can bring large companies under control, enforce strict regulations and even break them up. But modern technology companies are different from AT&T, and the same strategies that worked in the past may not apply today. The technology differs too much, but that does not mean lawmakers should abandon the idea of antitrust laws in the information technology space. Of course, there will be challenges, and understanding how modern monopolies differ will be crucial in overcoming those challenges. Some have suggested policy frameworks for similar antitrust legislation in the tech space that are worth consideration as to their potential effectiveness.

There is wide scale acceptance that traditional regulatory frameworks simply need to fit the current state of rapidly evolving technology. Belgian Law and Technology professor Carl Vander Maelen suggests that lawmakers use alternative regulatory institutions (ARIs) to deal with the changing nature. ARIs, as defined by Vander Maelen, are more reactive rather than proactive programs. In recognition that the slow moving process of government will never be able to keep up with the pace of innovation, any government program should leave space to update its institutions to meet the moment. Through a multi stakeholder approach, state and non-state actors can continuously meet at the negotiating table to update the rules within a larger framework.

One immediate benefit that jumps out from a flexible ARI framework is that it is best equipped to handle the global nature of technology companies. Alphabet , Amazon, Meta, etc, operate on a global scale. It is unrealistic to think that the policy of one single nation will fundamentally change their behavior and achieve the goal of protecting the right to privacy. An ARI system can offer universal codes of conduct that list values that apply to all companies that operate internationally should abide by while allowing each country to negotiate with the non-state entities on rules that may apply in their own country.

The question that should be asked when examining ARIs is whether codes of conduct, which are soft laws by nature, can translate into hard laws that compel private actors to comply. ARIs risk granting private actors too much power, allowing them to negotiate different rules with different states and elevating the status of the private companies to an almost nation-state-like status, which calls into question the notion of sovereignty, the very basis of the international system.

Dutch privacy law professor Anna Beckers believes this soft law can and will transform into hard law, promoting compliance with the codes of conduct. Specifically, in the European context, there has been a slow creeping juridification process of soft law codes of conduct becoming hard legally and socially binding laws. When a state has strong political and legal institutions, an issued code of conduct can be more effective. Through ensuring that a code is precise and spells out what is expected of private actors from a state, Beckers believes that the code, over time, will become normative and be the desired behavior.

If Becker's ideas are taken seriously, they could provide a framework for a policy regulating ubiquitous and transnational technology companies. Stating a list of values that a state expects a tech company to follow, like respect for an individual's privacy and an acknowledgment of the public utility quality of their services, we can imagine a world where all rights are to be respected. However, skepticism remains on the effectiveness of ARI's and code of conduct being able to carry the same legal weight as a legally binding, traditional top down, hard law legislation.

In opposition, data governance scholar Linnet Taylor believes that the economic power of technology giants has made them nearly impossible to regulate. In essence, Taylor argues that services provided by technology companies are so intertwined with public life that they have taken on the role of a public entity and must be treated as such. Private companies have more access to the population than governments, and even governments have come to rely on technology services provided by private companies to carry out their essential functions. Here lies the problem Taylor sees with all regulatory frameworks seeking to govern the technology industry. Companies have

begun to take on some government roles without the traditional checks and balances placed on a traditional state. An example of this given by Taylor is from the UK, where the government outsourced some of the tasks of its public national health service to Amazon to use its database to diagnose patients. As the public begins to accept the services provided by private sources of information as legitimate, there must be a conversation about accountability and transparency. Amazon, through their contract with the UK government, was under no obligation to make the database they used to make decisions public in the same way the government would be.

So, what is the solution to this problem of private companies acting as public entities without the same level of accountability. How do governments regulate industries and companies they have come to rely on. This section has provided an overview of what scholars such as Halavais, Moy, Becker, Taylor, and McCarthy have been discussing as theoretical frameworks for policy in the tech industry and a brief history of past strategies used by policymakers to attempt to regulate emerging technology markets.

Literature Review

Discourse on how new technologies create challenges for lawmakers

It is no secret that new technologies have revolutionized how we communicate, “Technological advances render unprecedented restrictions on privacy technically possible as well as economically affordable. The most important example is probably the Internet. Nowadays, human interaction takes place on the Internet significantly, as people communicate with each other and do their business online. Powerful organizations, including government agencies and companies, can keep track of these

interactions and combine them into a detailed picture of a person at a minimal cost. While the data-based profiling of customers by Internet companies and social networks, such as Alphabet or Meta, have long been the focus of the discussion, recent revelations have drawn attention to national intelligence agencies" (van Aaken,2014). Private actors have developed new technologies that have become too sophisticated for traditional forms of regulation and require governments to try and keep up. The question is if these new technologies are even possible to regulate. In the few years since the passage of the GDPR, there are questions about its ability to address the new challenges, " Apps continue to rely on tracking technologies, e.g., to retrieve analytics and show advertising, even after the introduction of the GDPR. The law does not appear to have changed these incentive structures fundamentally." (Kolling et.al, 2021). With new technologies making it easier for private companies to access the personal data of individuals, the importance of regulations has never been more apparent.

There is a general sense of fear and lack of understanding of how new forms of communications technology work and how they intrude on privacy, "the subjects of the conscious and unconscious negotiation make with networks, systems and the increasing levels of computational autonomy and authority that is in every sense alien and radically unknowable to the vast majority of users caught by and within them" (Herian,2018), " The spread of ubiquitous and pervasive computing collects a huge amount of personal data from online activities and mobile devices, intensify the threat for re-identification additionally. Ubiquitous devices such as smartphones and wearable badges, by utilizing a powerful set of sensors and utilities, can monitor biometric signals or location data of their holders to provide healthcare interventions or customized

driving directions respectively, thus assisting users in their daily tasks."(Politou, 2018). New technologies cause concerns among consumers and governments alike and started conversations about what is needed to protect the right to privacy, "a deep reflection is necessary about to what extent the normative side of the law should be transferred from the traditional 'ought to' of legal systems to automatic techniques through mechanisms of design, codes, and architectures" (Magrani, 134,2018). While innovative legal solutions have come about in recent years, there are concerns that these laws will not allow governments to keep up with decentralized, ubiquitous, and complex technologies.

Technologies such as the blockchain are creating alternative security protocols that differ from traditional digital technologies making it more difficult to track online communications and data extraction, which have made life difficult for regulators, "noting how their decentralized nature is likely to create difficulties for conventional lawmakers and enforcement officials in responding appropriately and effectively." (Yeung,2019).

Innovation in new technology has created a challenge for policymakers; the ubiquitous and transnational nature of data-sharing platforms has proven difficult to regulate by a single state. While the internet is not new, nor are regulations of activities that seek to monitor activities that occur there, instantaneous data sharing done on global digital platforms is still a challenge plaguing lawmakers (Wang, 2022). Platforms such as Alphabet, Meta, Apple, etc., operate in nearly every country in the world. Creating legislation to regulate their behavior would require a level of international cooperation never seen before. No government entity would seek to stifle the innovation

brought about by the giant platforms. However, there is the wish not to sacrifice the values states have built themselves on. “Society has to redefine the balance between privacy and other values, such as security or wealth, contingent on the opportunities and threats of the time, which include technological progress as well as other events” (van Aaken,2014).

Getting states to find policy solutions to the growing threat of privacy-violating technologies will be challenging. The international cooperation effort would prove extremely difficult due to differing value sets and definitions of privacy among states. Without an international agreement, we are left with a fragmented approach that does not provide clear guidelines to individuals on how their data is being privatized, as well as companies being unclear on their obligations to their consumers. “Companies have been faced with the dilemma of necessarily violating legal obligations of either one state or another, international data flows of great economic significance have been inhibited, and international relations have been jeopardized.”(Bougiakiotis, 2020). The logical solution would be to have all relevant actors come together, states and private companies alike, and come to an agreement that spells out the privacy rights given in the information age and what platforms must do to comply with these new regulations. Unfortunately, states' differing values regarding privacy would likely be too large of a gap to overcome to reach an agreement (Wang, 2022). An international agreement on privacy poses a different challenge than other global policy issues, as fundamental values vary, making it less likely for states to seek compromise. “However, in privacy matters, not only do states have their usual interests but also important social and legal values are at stake. Compromising on the rules would necessarily require the parties to

make concessions regarding fundamental values such as freedom of speech for the US and informational self-determination for the Europeans" (Bougiakiotis, 2020).

Even with the seemingly insurmountable differences in values, it does not mean the international community should not strive for a policy framework that protects the right to privacy and limits the power of global platforms. " The challenge to be grasped – and for which the traditional rules and principles that can be deduced from international and national law often appear inadequate and obsolete – is to harmonize conflicting interests and needs, such as data protection and global security, obtaining an adequate balance between market logic and the essential guarantee of prevailing and non-negotiable rights." (Maceranti, 2021).

As communication technologies and data-sharing platforms continue to advance rapidly, it is crucial to understand how that alters the public sacred relationship with the right to privacy and to continue to have conversations on how that relationship may change. Then policymakers need to understand how innovation has threatened the protection of privacy defended for decades and why there is a need to re-evaluate strategies.

Framing liberal ideas of privacy

The liberal world has wrestled with concepts of privacy for centuries, how to best protect individuals' privacy and what kind of laws need to be passed. However, the rise of digital technology has presented a new challenge in that fight. This section aims to understand how liberal minded countries, which will be defined as Western democracies that promote a capitalist economic structure, define and understand the idea of privacy

and, more specifically, data privacy—blending thoughts from scholars and politicians alike. This paper will seek to analyze European privacy laws in a later section so that understanding the basis on which the EU finds its legitimacy is crucial for analysis.

"Western states have sought to regulate first public and then private organizations' collection, storage, and sharing of personal information. Despite privacy being governable via constitutional law, privacy (also called data protection) laws were enacted to protect individual privacy rights" (Lippert, 2016). Privacy has also been called " arguably the most prototypical liberal right" (Raban, 2012) so understanding how liberalism, the ideology that is at the heart of European politics, sees privacy is essential to the analysis of privacy and data laws and the technology they seek to regulate.

Liberal minded scholars such as Ofer Raban, Randy Lippert, and Dominik Aaken have written about and have come up with no shortage of definitions for what privacy is and is not and how a liberal government should promote and protect the right to privacy. "Creating a free personal sphere where individuals pursue their personal well-being free from the coercion of others"(Raban,2012), "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"(Lippert, 331, 2016), " as a right to control one's access to oneself" (Aaken, 136, 2014), "private life is conceptually and institutionally distinct from the organs of collective decision and that, together, the two regions' functions compose the life of a democratic society" (Gerson, 2021). There are common themes: the definitions of privacy, the idea of individuals being in control, and freedom from government intrusion into personal life. The emphasis on individuals comes up so often in privacy laws in the liberal world that it is essential to explore. Still, although the

plethora of definitions cast a wide net over the concept of privacy, it is clear there is no universal agreement on the meaning of privacy. With such ambiguity, it is a difficult task for governments to create targeted legislation that can be effective in its goal of privacy, still, they try.

To understand privacy laws in liberal-minded governments, such as the EU, that have taken the definitions of privacy and applied them to the law, we must understand the logic behind the ideology. “The fundamental unit whose freedom is protected is the individual. The individual, not the marital unit or the family or one’s ethnic group, is the bearer of privacy rights. Liberal states prioritize the freedom and autonomy of individuals over the self-determination interests of any collective” (Raban, 1251,2012). Liberal societies and governments seek to free up individuals to pursue their own ventures in their life away from the interference of a regulatory agency, “Valuing individual liberty entails preserving it from the violent potential of politics, apparently necessitating the division between a private realm that allows scope for emotions, particular attachments, and subjective wishes, and a civic sphere which wields the collective instruments of enforcement” (Gerson,2021), “liberalism’s fundamental precept is the creation of a free personal sphere…within which actors freely pursue their personal welfare. Such a free personal sphere, free from public or private coercion, is purported to maximize personal prosperity” (Raban,2012).

Traditional debates on the definition and purpose of privacy have raged for generations. However, the discussion on defining and framing data privacy is much newer and needs more clarity. The digital information age has undoubtedly changed the way privacy is conceived, as the rise of large, global digital corporate platforms have

challenged the way privacy can be applied. “Given the global character of digitalization, together with its transnational technical infrastructure and ownership make-up, the relationship between digitalization, democracy, and privacy can no longer be conceived as being confined to nation-states” (Seubert and Becker, 2021). However, this challenge has not deterred liberal thinkers' commitment to the protection of privacy Liberal societies acknowledge that individuals are entitled to have control over their lives. In the data economy, this should include digital footprints, which are something like a cross between minute behavioral observation and DNA sequencing” (Ciocca, 2021). The move into the information age has created the need to redefine privacy, and just like the traditional debates on privacy, there is no one clear answer. To redefine privacy in the digital age, it is first necessary to acknowledge the actors responsible for the shift. We have to look at the global data sharing platforms, such as Alphabet and Meta, that created a business model that manipulates their users into sharing personal information and creates an environment where people come to rely on their services for their everyday needs, which is a direct challenge to the legal tradition of the protection of privacy (Tobert,2021).

Even with the challenge to privacy diagnosed, it does not mean scholars and policymakers agree on redefining privacy for the contemporary era. In the search for the meaning of privacy in the information age, there is the feeling that new privacy laws should not hinder the pace of progress in the development of new technologies and the freedom of expression that has benefited from the rise of new technologies (Shackleford, 2011). The insistence that progress should never be hindered in any circumstance is an essential feature of the neo-liberal ideology that created the

environment in which global digital platforms were allowed to flourish unregulated. However, many scholars and policymakers argue that a balance between continuing the tradition of privacy protection and innovation must be found. Ciocca suggests that any technology that seeks to manipulate human behavior violates the right to privacy under the liberal order, and it is necessary to regulate those companies. While others like MacCarthy argue that it is the role of the government to ensure that private companies operate in a manner that complies with the traditionally accepted definitions of privacy and is in line with the values of democracy. “A new privacy law would establish enhanced privacy duties for dominant technology companies to ensure that the consumer interest in effective data protection is vindicated in a context where consumers are less able to exercise their general privacy rights" (MacCarthy, 3, 2021). Regardless of how the right to privacy is understood, it is undeniable that the information age has changed how it is interpreted. The information age is still a relatively new phenomenon that policymakers are grappling with and are searching for the best solutions. For liberal governments who have based their ideology on human rights, equality, and freedom, it has been a struggle to keep up and deal with private companies that do not always share their values. Though it is imperative that liberal governments quickly find policy solutions to these new threats as it has, they can undermine their nation's security.

The regulatory response

So far, this paper has established the need for regulation in the technology industry from a scholarly perspective. Now, it is time to understand the lawmaker's perspective. Where do political and judicial officials see the need for regulations? This section will focus on the European perspective, as the European Union has been among the world's leaders in drafting innovative privacy policy solutions and has taken the challenge of updating its stance to meet the current state of technology seriously. Since the passage of the 1995 data protection directive, which was discussed above, the EU has been slowly tinkering with its standard for data protection. The EU has consistently shown its commitment to protecting individual privacy through court cases, laws at the national level, a series of nonbinding agreements, and culminating in the 2018 passage of the General Data Protection Regulation. The remainder of this section will trace the updates in policy and attitudes toward data protection between 1995 and 2018.

The first major milestone in privacy protection post-1995 came in 2000 with the EU-US safe harbor agreement. As per the ‘95 directive, the personal data of EU citizens could only be transferred to another country if that country had “adequate” levels of data protection. The United States Department of Commerce (DOC) and the European Commission reached an agreement where the DOC would provide a list of American companies that adequately adhered to the European level of data protection. Those approved companies would have been free from data blockages from the Europeans. The agreement was designed to continue to allow for Trans-Atlantic commerce to continue, as well as to bridge the gap between European and American notions of

privacy. The safe harbor agreement allowed American companies to continue the practice of self regulation, a feature of many American privacy laws, while allowing the Europeans to protect their state sovereignty and continue to carry out the tradition of stringent privacy laws and corporate skepticism. The safe harbor agreement is the first of many instances where the Europeans showed concern about threats to their national security and sovereignty from private companies. The agreement is also a starting point for the European's attempt to export their ideas and definitions of privacy to the rest of the world, a theme that will come up in other EU privacy laws that will be discussed.

The main feature of the safe harbor agreement that is key for analysis is that it allowed private companies to self regulate their compliance. Though the agreement was optional for American companies, many wanted to avoid losing out on the European market. Allowing for self regulation was a contributing factor for thousands of American companies to join the agreement. Nevertheless, the policy of self regulation was met with widespread criticism and legal challenges.

As early as 2004, the European Commission showed concern that many companies that agreed to the safe harbor principles were not fully compliant with the law. The 2004 annual compliance report stated, “The Commission services are concerned about the number of self-certified organizations that have not published a privacy policy or that have published a policy that is not compliant with the Principles”. Concerns and questions on the ability of the safe harbor agreement to properly enforce the European standard of privacy continued to plague the safe harbor agreement. A 2008 independent study concluded that only about half of the organizations signed up to the agreement provided adequate protection.

The concerns ultimately culminated in 2015 with a case before the European Court of Justice, which struck down the safe harbor agreement claiming that the self-certification process allowed in the agreement did not provide enough security for individual subjects, and American oversight bodies were not proactive enough in ensuring compliance. Ultimately due to the lack of privacy assurance, the safe harbor agreement conflicted with the 1995 data directive, which called for any data transferred to a third party country to be held to the same standards as it would be in Europe. The case was brought to the court by an Austrian privacy advocate who claimed Meta was not providing him with the level of protection required by EU law in the wake of the 2013 Edward Snowden case, which uncovered that American public authorities were scraping for personal data from social media platforms like Meta, including the data of EU subjects. American public authorities were not subject to the safe harbor agreement, so companies like Meta, who had signed on to the agreement, could not provide a safe harbor for the personal data of EU subjects. The court found that the mass surveillance programs run by U.S authorities were “incompatible with fundamental European rights” and that it is the role of the European privacy commission, under the ‘95 data directive, to independently examine each third country's compliance with the principles laid out in the law regardless of any other agreement made with that country. The court was left with no choice but to strike down the safe harbor agreement because American companies could not protect personal privacy equally.

After the European Court of Justice ruling, the state of international privacy agreements had become bare. It was becoming increasingly clear that old laws needed to be updated to align with the current state of technology. While discussions for

overhauling European data privacy policy had begun before the 2015 case, overturning the safe harbor law kicked talks up a notch as the urgency became more apparent with the revelations from the 2015 case. From here, the different stakeholders in the European Union began to negotiate a new law. However, with each country and regulatory body coming together with differing priorities and ideas, the process towards this new law was fraught with compromise and tense negotiations.

The European Union is a collection of nations that have come together to become stronger than they would be individually. Though that does not mean each nation agrees with each other on every issue, these disagreements were often displayed in the negotiations for a new data privacy law that ultimately became the GDPR. While Europe has always committed to protecting privacy, there are differences, sometimes subtle, in how the major EU stakeholders define privacy, like those defined in real world policy.

Beginning in France, where the protection of personal data processed in third-party countries is a matter of national security. The 2017 annual strategic review report named “ Disruptive technologies give rise to new opportunities and new vulnerabilities” as a vulnerability. Citing the lack of oversight on the web, France sees attacks through cyberspace as a potential threat to the nation itself. The review calls for a significant economic and political commitment towards developing new technologies that enhance France's ability to control what happens on the web concerning the activities of French citizens, calling the interference of other countries a violation of national sovereignty. Without this, France could be vulnerable to military attack. France

calls on its European partners to develop a policy framework to protect the union's security from outside sources who seek to violate their sovereignty.

The French are at the front in the fight against large technology companies' intrusion on the data rights of their citizens. French President Emanuel Macron stresses the need for “regulation that, on the one hand, creates an environment that encourages innovation, and, on the other, protects citizens against the power of the biggest platforms. In this respect, new rules are currently being implemented in Europe and at the national level.” The alarm is also raised about the need to protect national sovereignty from foreign corporations, especially American tech companies, and they want not to become a “digital colony”. The main conclusion and recommendations from the report are that there is a need to extend the ability of both French and European governments to regulate outside their borders and to be provided with more legal freedom to regulate any company that seeks to violate international sovereignty. Macron sees his role as an operator of the capitalist market of France while at the same time protecting the needs of French corporations and citizens.

Germany is another EU country with a strong tradition of passing laws and thinking about privacy. Shaped by the authoritarian nazi regimes of the past, the German public has been concerned with surveillance issues. Germans were so cautious of surveillance that the country did not have an official census until the 1980s, and this attitude has shaped how Germany has created privacy laws. In 2009 Germany updated its data protection act on top of the EU data protection directive, which they had agreed to. At the time, it was named the strictest privacy law in Europe. The law protects individuals from having their data processed by any public authority within

Germany. Criticism of this law comes from its inability to properly oversee the private sector and its limited scope of activities within Germany. Still, with the law's perceived shortcomings, it is a good insight into where the priorities of the German government lie when it comes time to negotiate and compared to those of other EU leaders.

Seeing the differences in philosophy and priorities among the leaders of different European countries, together to form a unified data privacy policy. The primary stated goal in passing a new law was to harmonize the regulations across the union, smoothing out the differing rules across the different countries. The challenge for lawmakers was finding common ground, seeing that the want to protect individual privacy is universal and not sink to the lowest common denominator. In the end, the leaders of Europe came up with the GDPR passed on April 14, 2016.

On May 25th, 2018, the GDPR officially replaced the 1995 Data protection directive passed by the E.U. The goal was to harmonize data protection across the EU as technology was now too unrestricted by national borders for different rules in different countries. The EU wanted to create a “ single digital market” beyond the union's borders. Any entity interacting with EU subjects will be required to follow GDPR rules. The GDPR sought to make guarantees for data protection and spell out fundamental rights. The law guarantees three rights; the right to be forgotten, the right to data portability, and privacy by design and default. The law was written in a manner that puts the primary burden on the companies who deal in the collection of personal data to operate with privacy as a priority and to set up their system to ensure compliance. Designing their product to remain as secure as possible is a priority that must be on par with its market viability. It goes so far as to require these companies to create a data

protection officer position, whose job is to ensure that the company is complying with the law and valuing the privacy of its customers.

The companies' responsibility is to set up the protective measures necessary to ensure privacy is protected as spelled out and that any new technology must be designed to protect privacy. It is a statement of values of how these companies ought to operate. The law calls for every company that deals with the processing and collecting of individual data to create a new position of Data Protection Officer to monitor the company's activities and report any violation of GDPR principles. Putting on one person or a small team is a big task. Requiring these companies to make changes in-house sets up a dilemma. While these companies may claim to value the privacy of their customers, ultimately, they are driven by profit and will inherently value that over anything else. The EU has its own enforcement mechanisms to ensure compliance from these companies. The EU will conduct assessments of companies; the one-stop shop allows each country to closely monitor the activity of a company within its borders to enable individuals to file complaints against companies for privacy violations. Any company found to violate GDPR rules is subject to fines and sanctions, which is hefty. 2% of worldwide revenue is no small thing.

With the framework and logic behind the passage of the GDPR, it is now time to take a closer look at the text of the law and break down individual articles that are most pertinent to the goals, as seen above.

Intentions of the GDPR

The following section looks at the texts and analysis of privacy theory and laws from around the world. It analyzes the intent of the legislation and then how they are to be implemented specifically in regard to the GDPR. It is essential to understand the dominant thought around data protection, what both governments and scholars believe needs to be done, and what has been done to prevent technology companies from outgrowing the reach of government regulation. An array of literature seeks to interpret the intentions of the GDPR.

The European Union is attempting to create a culture of compliance and privacy, where private companies value the individual right to privacy just as much as EU lawmakers do, whether through coercion or norm promotion (Zhang, 2021). In addition, there is a desire to create a market where European companies have a fair chance of competing with foreign competitors. The EU is exercising its right as the state as the primary regulator.

Belgian legal scholar Carl Van Der Maelen has looked at the measures put in place by the GDPR and sees the GDPR as the most innovative and substantial attempt to regulate private entities that reach across borders. Van Der Maelen acknowledges the challenges governments face in regulating modern-day multinational corporations and sees traditional regulation strategies as “ too rudimentary to adequately capture the complex interrelationships between state and non-state actors' (Van Der Maelen, 2020). Van Der Maelen calls the GDPR a new type of hybrid law that seeks to make the “codes of conduct” traditionally set up by regulatory laws more concrete and straightforward to enforce without a rigid top-down approach. Van Der Maelen sees the GDPR playing out

as a collaborative process between public and private actors, which many scholars see as a much more fluid process that allows the regulatory agencies to be much more capable of keeping up with the rapid technological change. It emphasizes that companies should adhere to the codes of conduct or norms set up by the law and encourages companies to follow them. “It posits broad hard law provisions and determines that codes are meant to specify those provisions by offering prescriptive and specific solutions that can result in compliance.” (Vander Maelen,2020)

Overall, Van Der Maelen raises important points surrounding the future of regulation in the information and communication technology sector and asks whether or not the text's existing laws need to be revised to meet the moment from the challenges of controlling transnational companies that can pick and choose which norms they follow to being able to understand the rapidly advancing technology. Van Der Maelen did not seek to offer solutions or pass judgment on the existing laws; he only sought to set the stage and acknowledge the nature of the new legislation. Other scholars seek to make predictions based on the text of laws such as the GDPR and how the institutions set up will operate.

Voss and Dumas agree on the potential effectiveness of the goals laid out by the GDPR and its compliance measures. Due to the newness of the law, which only passed in 2018, the debate is speculative and less evidence-based, and it will take more time to form proper conclusions, but that does not stop the debate from being any less heated. Voss and Dumas (2021) see the compliance mechanisms in the GDPR as a step towards protecting consumers' data and privacy, “the enforcement toolbox has expanded considerably, and collective action provides possibilities for individuals to

bring complaints more easily. In this context, this study now investigates strategic aspects and risks." Voss and Dumas believe that the threat of sanctions is strong enough to create a culture of compliance within the private sector that will allow for the GDPR to achieve what it set out to do, to stop the privacy violations of European citizens. " …companies (especially the U.S. Tech Giants) must ensure that their risk assessment tools are not too grounded in the past and adequately consider probable future changes. They should consider that big sanctions
that deter violations and demand compliance--are presumably on their way" (Voss and Dumas).

German data scholar Sebastian Golla does not share the confidence that the provisions of the GDPR will be enough to slow down private tech giants. There is a universal agreement that the GDPR is undoubtedly an improvement over past laws, but some worry that it needs to be revised to meet lawmakers' intentions. There is a lack of interest, awareness, and resources to control and stop data privacy breaches by tech companies (Golla, 2017). There is a concern that the Data Protection Agencies (DPA's) mandates are charged with the impossible task of being both a supervisory body that is supposed to work with and gain the trust of the technology companies to ensure compliance as well as the body that issues fines for non-compliance making it challenging to build that trust. While the GDPR and other data protection laws are still young, and it will take time to see how effective they are, it is important to remember why the EU passed these laws and how they have been set up to achieve success.

Policy Analysis of the GDPR

Intro to the GDPR

To understand how the values of privacy to the European Union are applied to action, the text of the GDPR must be scrutinized. On the surface, the legislation consists of 99 articles outlining the legal components of the, with an additional 173 recitals laying out how to comply with the law correctly. While some articles are carryovers from the previous generation of data privacy laws, a few seek to change how governments regulate the technology industry. The legislation's dense and often technical language can make it a daunting task for one to pick out which sections are the most fundamental to the new mission of the EU or which ones will prove to be the most controversial in their application. This section will highlight three of the most ambitious articles that seek to change the reality of the data privacy landscape. First is article three, which outlines the territorial parameters of the GDPR, giving the European Union authority outside of its borders and requiring any company seeking to do business in Europe to abide by the law. This is the EU attempting to export its privacy values to the rest of the world. Second, article six lays out the rights of the individual to control the processing of one's data. Laying the groundwork for the EU's view of privacy as an individual responsibility needed to be protected rather than a collective right. The third is Article 25, which seeks to instill the value of privacy by design and default into the everyday activities of technology companies. Article 25 projects to be among the most ambitious of the articles of the law as it seeks to change the way companies

operate from one of wide-scale data collection to one of adopting EU privacy values to their corporate culture. Analyzing the roots and logic of these articles will provide a picture of how European lawmakers intend to achieve the goals they set for themselves and maybe some insight into whether or not this law projects to be successful.

Before diving into the text of the law, a few terms that come up multiple times must be defined. Luckily EU lawmakers provided clear definitions for some of the most repeated concepts. First, the most common phrase is personal data. The EU defines personal data as “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factor, the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”. Next the GDPR provides definitions of activities taken by the companies. They separate processing which is defined as “ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction” and one who does those operations is known as the “processor” who is different from the controller who is known as “ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are

determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law”

Article three

The territorial scope of the GDPR is laid out within article three of the law. The text of the law states, “ (1)This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. (2)This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or(b)the monitoring of their behavior as far as their behavior takes place within the Union. (3)This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.” Article three is the most prominent example of European lawmakers attempting to control the state of privacy laws globally and not limiting themselves to only the borders of the EU. Forcing private companies to comply with this law, whether or not they are based in Europe, leaves them with no choice. The European market is simply too large for tech companies to ignore this law and miss out on the potential that lies on the continent. The stretching of the EU’s territorial jurisdiction raises questions surrounding international law. Does the European Union have the right to regulate non-European companies? If so, how will they do so, as cross-border enforcement is not a traditional form of regulation or the norm in international law?

Article three, most importantly, speaks to the ambition of the European Union to fundamentally change the privacy relationship between consumers and corporations and set the global standard of regulations. How the EU expects to effectively project its laws and values onto the rest of the world through article three is still being determined. The best those seeking to analyze the article can do is look towards the official guidelines that the EU has issued to clarify data processors. There is no better place to start analyzing the impact of this article than straight from the source of the lawmakers who passed the law.

A memo released by the EU data protection board states the intention of the article “Article 3 of the GDPR reflects the legislator’s intention to ensure comprehensive protection of the rights of data subjects in the EU and to establish, in terms of data protection requirement, a level playing field for companies active on the EU markets, in a context of worldwide data flows.” The memo acknowledges that the EU understands that it only has jurisdiction over the territory of EU nations and their citizens. However, it sets up the law to apply to any form of data processing that targets EU citizens regardless of where a company is based or where they locate their data processing activity. Widening territorial scope acknowledges what many in the technology field have noted for some time now, that the information age has made national borders less relevant as data freely flows across countries. Though the EU’s sovereignty is tied to the traditional concept of national borders, they nevertheless needed a way to achieve their goal of total data privacy for their citizens.

The question for EU lawmakers was then how to widen the territorial scope of the law while still respecting the traditional boundaries of sovereignty they are tied to. It took

a unique set of strategies to do so. The first clause of Article Three defines the criteria for establishing data processors and controllers. The clause defines establishment not as being physically located within an EU member state but as “ the effective and real exercise of activities through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.” For the EU, a “ stable arrangement” can be as little as a single employee working with a European entity regularly. However, there are some exceptions to the establishment criteria. For example, for a controller to be subject to GDPR rules, the text states that data processing activities done “ within the context of EU establishment” are subject. Meaning only if the processing of personal data is linked to the company's activities within EU member states the GDPR applies. Still, if the presence of a company within the EU results in no data processing, then the GDPR does not apply; the EU evaluates activity on a case by case basis.

The language of the first section of article three asks data controllers to be careful and evaluate their activities with the EU. However, there are concerns about the abilities of both lawmakers and controllers to determine whether or not being established within the union directly accurately leads to the processing of personal data, especially for larger companies that deal with a large amount of data that freely flow across borders. The criteria for establishment could be clearer.

The second clause of article three further complicates the territorial scope of the law by establishing criteria for targeting data subjects. The law states that the GDPR will apply to controllers who offer goods and services to data subjects when such activity occurs within EU territory, regardless of the subject's nationality or where the controller

is located. The text provides a broad and vague definition of targeting as any activity targeting EU subjects with goods or services specifically tailored for the European market, whether through the use of a European language or accepting a European currency. Even if the controller has established itself outside of the union and is located in a non union country, it will still be subject to the GDPR. The law also protects non-EU citizens while in the union the guidelines give the example of a mapping app that provides guides for tourists while visiting cities around the world; if that app offers a guide for a European city, the GDPR sees that as targeting, and the law will be applied.

The second clause further widens the territorial scope of the law as it seeks to bring foreign and non European companies into compliance. It is a break from traditional forms of regulation. However, even as the EU tries to make territorial scope, there are still questions about the ability of lawmakers to do so and how the EU expects to control the activities of non-European companies.

A unilateral expansion of territoriality is seen as a direct violation of sovereignty as defined by international law. By expanding territoriality into other countries, the EU is running the risk of creating confusion for foreign controllers and processors who already have to comply with the laws of their own country but now have to be aware of the laws of the European Union.There is also the risk of contradiction between the laws of different countries, in that case, it needs to be clarified which law controllers and processors should follow without running the risk of being in violation and fined. This puts an excessive burden on individuals and companies, with so many variables that go into determining where and when the extraterritoriality of the GDPR comes into play, it will be difficult for both individuals and companies to understand when they need to

comply. Especially for individuals who may need to be better informed about minute details of data privacy laws may not always be aware of when their rights are being protected.

In an age of globalization, companies have data processing operations around the world. With article three's language, the EU expects these companies to change their worldwide behavior based on their values. For example, say there was an American-based company that targets users' data from around the world, including EU countries, and processes that data back in the United States. The company is not explicitly targeting EU subjects, but the language of the GDPR stipulates that this company would need to comply with all of the law's components. The question arising from this situation is whether or not the EU has the legal right and legitimacy to change the behavior of a foreign company.

The third and final point of the implications of article three is the value exportation that the EU is doing. It has been established that the goal of European lawmakers in writing this law was to protect the right to privacy for individual subjects. There is the question of whether or not the EU has the right to enforce those values on non-EU subjects, foreign governments, or companies. The current state of international law is based on respect for other countries' sovereignty and laws. However, article three has sought to reach into the territory of other countries. Proponents of the extraterritoriality clause would cite how the need to regulate the extraction of individuals' data is a global issue. With no universal law anywhere, there needs to be someone who takes the first step toward putting checks on private technology companies. It also speaks to Europe's ambition to become a regulatory superpower; if they can set the rules of business, they

can project their power onto the world. Article three may be the first step toward motivating other countries to pass similar laws to GDPR and creating an international standard for data protection, or the future may consist of differing laws creating confusion for both controllers and processors as well as individuals as to how to comply with the differing laws and values of states properly.

Article Six

The second in the group of articles that are critically important to the mission of the GDPR is article six. Article six defines acceptable conditions in which a controller can process an individual's data. There are several situations that article six lays out for good terms for data processing. The first is consent individuals must give controllers their approval to process their data. An example of this is when you enter a website, and there is a prompt that asks if you accept cookies storing your personal information on that site, that is article six in action. There is also data processing to carry out a contract that an individual has knowingly entered. Finally, and perhaps most consequently, article six allows for " processing is necessary for the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child". The most important term to understand in that clause is "legitimate interest." Unfortunately, the text of the legislation provides no clear definition of what is supposed to be meant by a legitimate interest, so to try and understand this concept, we must turn to legal scholars and other governmental bodies to provide clarity.

The United Kingdom's Information Commissioner's Office published guidelines to clarify article six. First, the guidelines outline a three-part test to ensure that processors align with the law. Controllers must ask themselves if processing an individual's data has a purpose that will directly lead towards achieving their legitimate interest, whether or not that data processing is necessary. Finally, the interests of the individual whose data is being processed must be considered and balanced with the controller's interests.[1]

The guidelines give one concrete example of what may count as a legitimate interest for a controller to process personal data; an insurance company (the controller) needs to process their customers' data to spot fraudulent claims. Article six sees this form of processing as a legitimate interest of the insurance company. The company proved it had a business reason to process its customer's data. They had also proven that this activity was necessary to their legitimate interest and could only have achieved their interest with data processing.

The last component in understanding legitimate interest is the need to balance the interests of controllers and processors with the interests of individuals. As this law is about protecting individuals' rights, each article must include provisions targeted at that goal. The UK guidelines state, " The balancing test is where you take into account the interests or fundamental rights and freedoms of the data subject which require the protection of personal data"[2]a check on controllers and processors so they do not override the rights and interests of the individual. In essence, this is a light-touch risk assessment to check that any risks to individuals' interests are proportionate. In other

[1] "What Is the 'Legitimate Interests' Basis?," ICO, accessed April 11, 2023, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/.
[2] See footnote 28

words, if the processing of personal data prohibits an individual from exercising their rights laid out in other sections of the law, then the individual's interest outweighs the interest of the processor and is considered a violation of the law and the fundamental right to privacy.

Even with the guidelines, the language of article six still leaves room for interpretation; who is the judge of when the interest of an individual outweighs a processor or when the processing of personal data is essential for a controller to achieve their interest? There is an understandable weariness of the vague language of the law and the want to seek more clarity and suggestions.

Data law scholar Fabrizio Espositio is concerned with the balancing test that the EU created as the basis for determining the legitimate interests of both controllers and consumers, mainly if a data subject decides to exercise their right to opt out of having their data processed, which is enshrined under article 6(1A) will they be at a disadvantage in their economic activity online, if a consumer or data subject can prove they have a legitimate interest in not having their data processed they can't stop controllers from doing so. Esposito asks if consumers/ data subjects be retaliated against for not giving their consent to processors and be offered higher prices on goods they seek to purchase, which he calls the "impersonal price." Data processors altering the price of the product they sell based on the consent status of a consumer is a concern and undermines the whole project of the GDPR to take back the controls of individual personal data. Article six enshrined the right for consumers to opt out of data processing programs run by nearly every internet company and made consent the fundamental legal instrument for protecting consumers. Esposito concludes that "the

GDPR contributes to a trustworthy digital environment for consumers and a level playing field for traders, which stimulates competition on the merits" and that provisions within article six, as well as others, are sufficient for protecting the rights of consumers who chose to opt out of personalized data processing to be offered a similar experience as those who do choose to give consent for their data to processed and received a personalized price on goods and services."

Esposito may be putting too much faith in the willingness of private companies, who are motivated by profit above all, to create a level playing field for all, regardless of their consent status for processing. The ability of the EU to enforce these regulations remains to be seen, and more research will be required. However, the state of technology makes it difficult to see how full enforcement is possible. The code and algorithms are too complex and abstract for most to understand and too ubiquitous to be targeted for regulation. For the goals of article six to be achieved, there must be a culture shift within private companies to one where the right to privacy is as much of a priority as making a profit.

Article 25

It is the opinion of this paper that no aspect of the GDPR makes a more ambitious attempt to protect the right to privacy in the information age than Article 25. The goals of the previously discussed articles and the entire mission of the European Union are rendered irrelevant without proper enforcement of Article 25. Entitled "privacy by design and default," article 25 seeks to change the priorities of private companies to value the right to privacy in the same manner as the EU. The key points from the text of the article are " the controller shall, both at the time of the determination of the means

for processing and at the time of the processing itself, implement appropriate technical and organizational measures… to meet the requirements of this Regulation and protect the rights of data subjects) (25-1), “ The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed” (25-2), as well as “ In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default.” (recital 78). Article 25 requires data processors and controllers to consider the nature and scope of their data processing activities and how those activities may threaten individuals' rights. It states that processors must structure their organizations to prioritize privacy rather than an afterthought.

The great strength of Article 25 is that it seeks to create a proactive approach to data protection. In its best form, processors will always have individual rights in mind. It can promote transparency between organizations and individuals and hold those who violate the right to privacy accountable. Article 25, in essence, is the mission of the European Union in writing this law, to create a world where the commitment to the right to privacy is a central pillar.

To understand Article 25, first, its legal heritage must be traced. The idea of privacy by design and default did not originate in the GDPR but has been a primarily European legal concept. Article 25’s antecedent exists in the 1995 EU DPD, which states in recital 46 of the law, “ Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate

technical measures be taken, both at the time of the design of the processing system and at the time of the processing itself". The language in the data directive does not go as far as the language of the GDPR, the new law adds organizational measures, not only technical ones. The process from Recital 46 of the DPD to Article 25 of the GDPR is a long and winding road that spans the laws of multiple countries and court cases at the highest levels of the European justice system.

In 2008 the European Court of Human Rights ECtHR) heard the case of i v. Finland. The plaintiff, a woman identified as "i" for privacy concerns, claimed that the hospital treating her for HIV had violated her right to a private life under Article 8 European Convention for the Protection of Human Rights and Fundamental Freedom (ECHR). The complaint was based on the hospital's failure to create a system that ensured her patient record was secure. While Finnish law and hospital policy had provisions in place designed to protect from a privacy breach, the court ruled they did not go far enough " The Court notes that the mere fact that the domestic legislation provided the applicant with an opportunity to claim compensation for damages caused by an alleged unlawful disclosure of personal data was not sufficient to protect her private life. What is required in this connection is practical and effective protection to exclude any possibility of unauthorized access occurring in the first place. Such protection was not given here". The gist of the ruling is that the protection of personal data is a basic human right, and the Finnish law simply did not go far enough to protect that right that hospitals needed to place a higher priority on protecting their patient's right to privacy. Again, this ruling still does not go as far as Article 25, but it establishes the right to *de facto* right to privacy and is under the same logic as Article 25.

Article 25 jumps from previous legal precedents because it requires organizational measures to be put in place to protect privacy, not just technical ones. Every decision a processor of personal data makes, whether it be a hospital, private company, or government body, must keep protecting the right to privacy at the top of mind, or in other words, by design and default. In short, in the words of Norwegian computer law expert Lee Bygrave, " The overall thrust of GDPR Article 25 is to impose a qualified duty on controllers to put in place technical and organizational measures designed to implement data protection principles effectively and to integrate necessary safeguards into the processing of personal data". Article 25 expects businesses to include privacy into their core strategies, not only to create systems of privacy within their products but to have it permeate into every level of their organization.

Even with establishing the precedent and logic behind Article 25, there are doubts about its legal standing and effectiveness in creating a culture where privacy is by design and default. There are concerns about the vagueness of the language written in the article. No clear directives are written anywhere in the GDPR or related directives that give tangible examples of what, by design and default, truly means.

Law professor Ari Waldman calls article 25 " hopelessly vague," allowing too much room for interpretation to be enforced. Instead of being a clause designed to transform how we expect businesses to conceptualize privacy, it is simply a reminder to comply with the other parts of the law. Although, as already established, there is no clear and universally agreed upon definition for privacy, the language of article 25 provides no clarity on what definition this law uses. Allowing each public and private organization to operate based on its definition of privacy. Fears of inconsistent

enforcement and a lack of genuine commitment to implementing privacy by design and default are valid.

Bygrave points out that the vagueness of Article 25 can be attributed to the lack of conversation between lawmakers and those who work for data controllers has led to a disconnect between the two groups. For Article 25 to be effective, it would have been in the best interest of lawmakers to include all of the relevant stakeholders in the creation process. It could have led to a more energized and willing partnership between private and public. The lack of inclusion of the private sector in the creation of the law only makes sense if European lawmakers believed that the private sector had no interest in creating a culture of privacy by design and default. There is a history of private technology companies creating their privacy policies attempting to protect the right to privacy of their consumers. The criticism of allowing private companies to police themselves is that they have built their entire business model of processing personal data and making a profit from it; it is how they survive. It would be impossible for an entity that has built its entire existence off the processing of personal data and the violation of the long held tradition of the right to privacy to commit to privacy by design and default entirely. Thus the need for Article 25 to be led by a body dedicated to the mission of privacy by design and default is found.

The passage of article 25 can be credited for putting the idea of privacy at the top of mind for controllers and those who design products for technology companies. No company wants to get fined for violating the law, and to avoid those fines, companies must consider privacy. At the very least, conversations are happening on how to best design products with privacy as the default, and over time more innovative strategies on

how to best go about that will come about. Whether or not companies commit to developing these products remains to be seen, the idea of privacy by design and default is now no longer a chatter of the legal community but a topic of public discussion, which can be credited to Article 25.

Like every aspect of this law, the privacy community is still in wait-and-see mode on the future effectiveness of Article 25.

Compliance

This paper has provided a clear background and theoretical basis for the issue of the right to privacy in the information age, from understanding how scholars and lawmakers alike have come to understand privacy to how that understanding has translated into real-life policy decisions. Until this point, this paper has provided an informational and analytic perspective on the state of the right to privacy in this age. Much has been made about companies' efforts to regulate privacy invading technologies, but it is crucial to understand if those efforts are successful. Unfortunately, defining success in this field is not easy, as established privacy is difficult to define and there is no statistic to measure it. So, how can we conclude the effectiveness of the GDPR and the state of the right to privacy?

There are a few factors to look at. First, we can evaluate the enforcement measures the EU is taking to ensure compliance with the law. One of the most pressing challenges at the passage of the GDPR was how the EU was going to convince non European companies that they needed to comply with European law. With most of the

large tech companies being based in the United States, the EU needed to devise a strategy to monitor their activities and enforce sanctions when necessary.

On September 1, 2022, the European Union opened an office in San Francisco which in the words of Josep Borrell, the high representative of the union for foreign affairs and security policy, the office is designed to " reflect the EU's commitment to strengthen transatlantic technological cooperation and promote a global digital transformation based on democratic values and standards". This is a concrete step in deepening the EU's work in cybersecurity, countering hybrid threats, and manipulating foreign information and interference". The keywords to focus on in this statement are "democratic values." In the analysis of the legislative text section, the exportation of values in article six was discussed, and how the EU attempted to create an extraterritorial policy framework to ensure their definition of privacy and standards of protection are respected around the world. The European Union, a government body based on the ideas of democracy and the rule of law, is with the GDPR trying to ensure control over the basic personal information of EU subjects away from private actors who are not bound by the same values of the state, despite their state-like power. Again we see Europe projecting its regulatory power onto the world to advance its national interests.

It is not unreasonable for the EU to feel they needed to be close to the source of the problem as they see it. With the office being located in San Francisco, they are within a one hour drive to the headquarters of some of the largest data extraction companies in Alphabet, Apple, and Meta. It sends a message to these companies that the EU is serious about its efforts to enforce privacy standards around the world. It is

also an opportunity for the Union to clarify the GDPR, which, as discussed, is plagued by its vagueness and fosters a more productive relationship between regulators and companies. The office's opening could also indicate that the EU does not believe it can regulate these companies from across the Atlantic. They struggle to enforce their extraterritoriality and promote a culture change within private companies. At the time of writing this, the office in San Francisco is less than six months old. It has not made any significant decisions; it would be unfair to judge how effective it will be in enforcing GDPR compliance and even how exactly it aims to do so. In the future, the activities office may be an effective indicator of enforcement and compliance, but for now, other factors must be more seriously considered.

Another way to measure effectiveness is by looking at how other governments have responded to the GDPR, whether they have passed countermeasures or created companion legislation with similar aims. Comparing other countries' legislation is a good indicator of the momentum in data privacy and whether the GDPR is set to become the new standard of data privacy legislation or will be seen as more of an outlier.

As of now, there is more evidence pointing to the GDPR being only the first piece of legislation in a new generation of data privacy laws seeking to change the way businesses are allowed to process personal data as a wave of new laws has been passed in an attempt to set a similar standard. Starting in California, the state has passed its own law explicitly modeled after the GDPR. The California Consumer Privacy Act (CCPA) seeks to increase consumer transparency over how businesses collect their data. Only applying to those who reside in California, the CCPA differs from the GDPR in that the CCPA only applies to large for profit companies and allows individuals to

opt-in or out of allowing companies to process their data, compared to the GDPR, which applies to all businesses around the world and gives no choice of opting out. Overall the law seeks to achieve the same goal, even the differences in some of the smaller details, to allow the data subject more transparency and control over how their data is processed.

On a national level, the United States has attempted to rework the safe harbor agreement that the CJEU struck down on the basis that US privacy standards were not on par with European standards. On October 10, 2022, President Biden issued an executive order mandating that U.S intelligence agencies create a new framework where they may only conduct data gathering operations that are strictly necessary for national security and do not impact individual civil liberties. The EU has yet to decide on whether or not the renewed commitment to privacy by the US is adequate in its protection standards and if it will lead to a new agreement between the two governing bodies.

The EU has become the leader in privacy policy as more and more countries pass laws in the same vein as the GDPR. In terms of creating a strong regulatory environment around privacy, the GPPR should be considered a success, but that does not mean private companies have complied with the new law. Despite the law's short lifespan so far, it is worth investigating how private companies have reacted and if they are truly changing their attitudes on privacy to match those of the EU.

Measuring the success of a law only five years after its implementation, especially one as complex and far reaching as the GDPR, is a difficult task and possibly not a fair one either. However, it is worth exploring the changes the law has made, if

any, in the world of data privacy in its short life in the private sector, and can be a good indication of what is to come in the future.

The Center for international strategic studies reports that the EU has issued a total of 839 fines for non-compliance through the end of 2021. The highest number of fines were issued due to " insufficient technical and organizational measures to ensure information security." Of course, this statistic can be read in two ways, first that the EU is being proactive in the early stages of this law to set a standard of expectations for companies that the rules are to be followed, or that a large number of fines is an indication of companies not feeling the need to comply.

Some are concerned that no matter how well written the law is or how strong enforcement techniques are, the challenges posed by modern technologies are too advanced for regulators to keep up. Mone and Sivakumar point out how the values laid out in the GDPR, transparency, lawfulness, data minimization, purpose limitation, and accuracy, are the antithesis of how these companies built themselves up. The data extraction and processing systems are so ingrained in the operations of so many companies that complying with the rules of the GDPR would be harmful to business, making it extremely difficult for companies to value complying.

It is a balancing act that the EU has to reckon with; on the one hand, it is true that stifling the innovation of these companies should not be the goal in recognizing the good some of the technologies they developed brought to the world. On the other hand, the values of privacy, state sovereignty, and controlling corporate greed must be the priority of the Union. The Union must stand firm and enforce compliance with the

regulations they set out; they can not allow for the technology industry to continue with their practices of wide scale privacy invasion.

Conclusions

This paper has examined the struggle between nation-state and private corporate power, and the policy solutions offered by states to address this struggle. The European Union's General Data Protection Regulation is the single most ambitious policy by a government body seeking to set the rules of business in the digital sphere and ultimately maintain supremacy over corporate interests. The question remains if the GDPR, and those it inspired will truly offer a long term solution to continue the mission of protecting privacy and democratic institutions. Ultimately time will be the judge of that question for now the EU has moved the conversation in the right direction.

Europe has attempted to project its power through law and become a regulatory superpower by projecting its values onto the world, specifically in the digital sphere. This paper has established access to information as a legitimate source of power. With the GDPR The European Union is attempting to set the rules for how personal information ought to be dealt with. If the EU is successful in setting the rules for engagement for business and establishes itself as the main regulator for the technology industry it will position itself as a powerful force in the global economy and politically.

To set the rules on how the asset of personal data ought to be dealt with. Europe is reclaiming its sovereignty from technology companies. By leading by example, Europe is leading the way in the fight to protect privacy which will only raise

the standing of the EU on the global stage as the encroachments of technology companies begin to become a global priority.

It is unrealistic to believe that a single policy from a single entity will be able to rewrite the rules for data privacy globally. It will take a world wide collaborative effort to stand up to the practices of data extracting corporations. While as established there are other governments who have followed the lead of the EU there is still a long way to go and differing values among different countries continues to be a hurdle in creating a global framework regulating data privacy.

What the EU and the GDPR can take the most credit for is that there is now no shortage of media outlets, scholars, activists, and lawmakers discussing the effects of private technology companies being allowed to operate completely unregulated. An institution as influential as the European Union taking such a strong stance will only move the conversation forwards. The GDPR is flawed, mainly its unclear wording and inconsistent rulings. Still, the message is clear; the European Union will not stand for the undermining of democracy and state sovereignty.

The underlying theme to all of the discussions is how to protect the right to privacy that has been a staple of Western, capitalist, democracies for generations. Much like other rights, privacy must be constantly defended as always by those who seek to take it away. Whether it is through state policy or the conscious decisions of individuals, privacy is right that all be aware of, understand its value to living a free and comfortable life and be ready to defend it.

References

, 2017 French Strategic Review of National Defense (n.d.).

3 years later: An analysis of GDPR enforcement: Strategic technologies blog. CSIS. (n.d.). Retrieved April 28, 2023, from https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement

Andrew, J., & Baker, M. (2019). The General Data Protection Regulation in the age of surveillance capitalism. *Journal of Business Ethics*, *168*(3), 565–578. https://doi.org/10.1007/s10551-019-04239-z

Atske, S. (2022, May 11). *Social media use in 2021*. Pew Research Center: Internet, Science & Tech. Retrieved April 28, 2023, from https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/

Beckers, A. (2018). The creeping juridification of the code of conduct for business taxation: How eu codes of conduct become hard law. *Yearbook of European Law*, *37*, 569–596. https://doi.org/10.1093/yel/yey006

Black, S. K. (2002). The Telecommunications Act of 1996. *Telecommunications Law in the Internet Age*, 55–98. https://doi.org/10.1016/b978-155860546-6/50025-9

Bougiakiotis, E. (2019). The layered links model: An alternative approach to International Privacy Regulation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3464380

Bygrave, L. A. (2017). Data protection by design and by default : Deciphering the EU's legislative requirements. *Oslo Law Review*, *4*(2), 105–120. https://doi.org/10.18261/issn.2387-3299-2017-02-03

Chapter 2 - Background. Monopoly Asserted -- 1918-1934 | History of Computer Communications. (n.d.). Retrieved April 28, 2023, from https://historyofcomputercommunications.info/section/2.8/monopoly-asserted-1918-1934/

ciocca, paolo, & Biancotti, C. (2019). Data Protection and the future of Liberalism. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3726847

Cohen, J. (2013). What is Privacy For. *Harvard Law Review*, *126*(7), 1904–1933.

Data Protection Law: How it all got started. Data Catalyst. (2020, June 23). Retrieved April 28, 2023, from https://datacatalyst.org/reports/data-protection-law-how-it-all-got-started/

Data protection. European Commission. (n.d.). Retrieved April 28, 2023, from https://ec.europa.eu/info/law/law-topic/data-protection_en

de Hert, P., & Czerniawski, M. (2016). Expanding the European Data Protection Scope Beyond territory: Article 3 of the General Data Protection Regulation in its wider context. *International Data Privacy Law*, *6*(3), 230–243. https://doi.org/10.1093/idpl/ipw008

Esposito, F. (2022). The GDPR enshrines the right to the impersonal price. *Computer Law & Security Review*, *45*, 105660. https://doi.org/10.1016/j.clsr.2022.105660

Fact sheet - senate. (n.d.). Retrieved April 28, 2023, from https://www.commerce.senate.gov/services/files/1DEDF0BE-B800-4A47-A625-816CD85BC05A

Galexia. (n.d.). *Galexia internet*. Galexia. Retrieved April 28, 2023, from https://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/

Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - version adopted after public consultation. Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - version adopted after public consultation | European Data Protection Board. (2019, November 12). Retrieved April 28, 2023, from https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en

HALAVAIS, A. L. E. X. A. N. D. E. R. (2000). National borders on the World Wide Web. *New Media & Society*, *2*(1), 7–28. https://doi.org/10.1177/14614440022225689

Herian, R. (2020). Blockchain, GDPR, and fantasies of data sovereignty. *Law, Innovation and Technology*, *12*(1), 156–174. https://doi.org/10.1080/17579961.2020.1727094

i v Finland (European Court of Human Rights July 17, 2008).

Jasmontaite, L., Kamara, I., Zanfir-Fortuna, G., & Leucci, S. (2018). Data protection by design and by default: *European Data Protection Law Review*, *4*(2), 168–189. https://doi.org/10.21552/edpl/2018/2/7

Lex - l14012 - en - EUR-lex. EUR. (n.d.). Retrieved April 28, 2023, from https://eur-lex.europa.eu/EN/legal-content/summary/protection-of-personal-data.html

Lippert, R. K., & Walby, K. (2013). Governing through privacy: Authoritarian liberalism, law, and privacy knowledge. *Law, Culture and the Humanities*, *12*(2), 329–352. https://doi.org/10.1177/1743872113478530

MacCarthy, M. (2020). Enhanced privacy duties for dominant technology companies. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3656664

Maceration, A. (2021). New technologies between law and ethics: Some reflections. *Białostockie Studia Prawnicze*, *26*(3), 9–24. https://doi.org/10.15290/bsp.2021.26.03.01

Magrani, E. (2017). Threats of the internet of things in a techno-regulated society. *ACM SIGCAS Computers and Society*, *47*(3), 124–138. https://doi.org/10.1145/3144592.3144604

Mansell, R. (n.d.). *Are we losing control? - iicom.org*. Retrieved April 28, 2023, from https://www.iicom.org/wp-content/uploads/4-7-digital-divides.pdf

Mone, V., & Sivakumar, C. L. V. (2022, November 28). *An analysis of the GDPR compliance issues posed by New Emerging Technologies: Legal Information Management*. Cambridge Core. Retrieved April 28, 2023, from https://www.cambridge.org/core/journals/legal-information-management/article/an-analysis-of-the-gdpr-compliance-issues-posed-by-new-emerging-technologies/1E6F90DEDDDA1AA60A7912A162C00928

National laws. (2020). *Data Protection, Privacy Regulators and Supervisory Authorities*. https://doi.org/10.5040/9781526514240.chapter-003

OECD Legal Instruments. (n.d.). Retrieved April 28, 2023, from https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

Opening of the European Union Office in San Francisco. Consulat Général de France à San Francisco. (n.d.). Retrieved April 28, 2023, from https://sanfrancisco.consulfrance.org/opening-of-the-european-union-office-in-san-francisco#:~:text=The%20European%20Union%20opens%20on,in%20the%20digital%20technology%20secto

O'Hara, K. (2020). Big Data, consequentialism and privacy. *Big Data and Democracy*, 13–26. https://doi.org/10.3366/edinburgh/9781474463522.003.0002

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/cybsec/tyy001

Raban, O. (2012). Capitalism, Liberalism, and the Right to Privacy. *Tulane Law Review*, *86*.

Schackleford, S. (n.d.). *DEFINING PRIVACY IN THE INFORMATION AGE*. Arizona State Law Journal.

Schrems v Data Protection commissioner (High Court of Ireland October 6, 2015).

Search engine market share worldwide. StatCounter Global Stats. (n.d.). Retrieved April 28, 2023, from https://gs.statcounter.com/search-engine-market-share

Seubert, S., & Becker, C. (2021). The Democratic impact of strengthening European Fundamental Rights in the digital age: The example of privacy protection. *German Law Journal*, *22*(1), 31–44. https://doi.org/10.1017/glj.2020.101

Taylor, L. (2020). Public actors without public values: Legitimacy, domination and the regulation of the technology sector. https://doi.org/10.31235/osf.io/gtw2x

Torbert, P. (2020). Because it is wrong: The immorality and illegality of the online service contracts of Google and facebook. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3537227

Universal declaration of human rights - english. OHCHR. (n.d.). Retrieved April 28, 2023, from https://www.ohchr.org/en/human-rights/universal-declaration/translations/english

van Aaken, D., Ostermaier, A., & Picot, A. (2014). Privacy and freedom: An economic (re-)evaluation of privacy. *Kyklos*, *67*(2), 133–155. https://doi.org/10.1111/kykl.12047

Vanberg, A. D. (2020). Informational privacy post GDPR – end of the road or the start of a long journey? *The International Journal of Human Rights*, *25*(1), 52–78. https://doi.org/10.1080/13642987.2020.1789109

Vander Maelen, C. (2020). From opt-in to obligation? examining the regulation of globally operating tech companies through alternative regulatory instruments from a material and territorial viewpoint. *International Review of Law, Computers & Technology*, *34*(2), 183–200. https://doi.org/10.1080/13600869.2020.1733754

Vedova, H., & Technology, T. F. T. C. O. of. (2022, March 4). *The antitrust laws*. Federal Trade Commission. Retrieved April 28, 2023, from

https://www.ftc.gov/advice-guidance/competition-guidance/guide-antitrust-laws/antitrust-laws

Vincent, J. (2019, July 10). *Amazon's Alexa will deliver NHS medical advice in the UK*. The Verge. Retrieved April 28, 2023, from https://www.theverge.com/2019/7/10/20688654/amazon-alexa-health-advice-uk-nhs

Waldman, A. (n.d.). Data Protection by Design? A Critique of Article 25 of the GDPR. *Cornell International Law Journal*, *53*(1), 147–167.

Wang, J. (2022). The best data plan is to have a game plan: Obstacles and solutions to reaching International Data Privacy Agreements. *Michigan Technology Law Review*, (28.2), 385. https://doi.org/10.36645/mtlr.28.2.best

What is the 'legitimate interests' basis? ICO. (n.d.). Retrieved April 28, 2023, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/

Yeung, K. (2019). Regulation by Blockchain: The emerging battle for supremacy between the code *of* law and code *as* law. *The Modern Law Review*, *82*(2), 207–239. https://doi.org/10.1111/1468-2230.12399

Zhang, Y., Wang, T., & Hsu, C. (2019). The effects of voluntary GDPR adoption and the readability of privacy statements on customers' Information Disclosure Intention and trust. *Journal of Intellectual Capital*, *21*(2), 145–163. https://doi.org/10.1108/jic-05-2019-0113