A general approach on privacy and its implications in the digital economy

Mariola Sánchez-Romero*

December 1, 2021

Abstract

The information age sets off a revolution for organizations and institutions without precedent. Big production of data is a major competitive advantage for companies. Therefore, there are great economic incentives to monetize such data. However, there is evidence that indicates clear vulnerability in terms of user privacy, thereby setting a new paradigm in the search for a balance between privacy and security. This article offers a brief history of privacy to this day, deepens in the scope and importance of its standardization in the regulation and future of digital markets.

Keywords: Privacy, Markets for personal data, Regulation

*The author thanks Amparo Urbano for her comments and suggestions. Department of Economics and Financial Studies, Miguel Hernández University. Avda. de la Universidad s/n, E-03202 Elche Spain. e-mail: mariolasr14@gmail.com

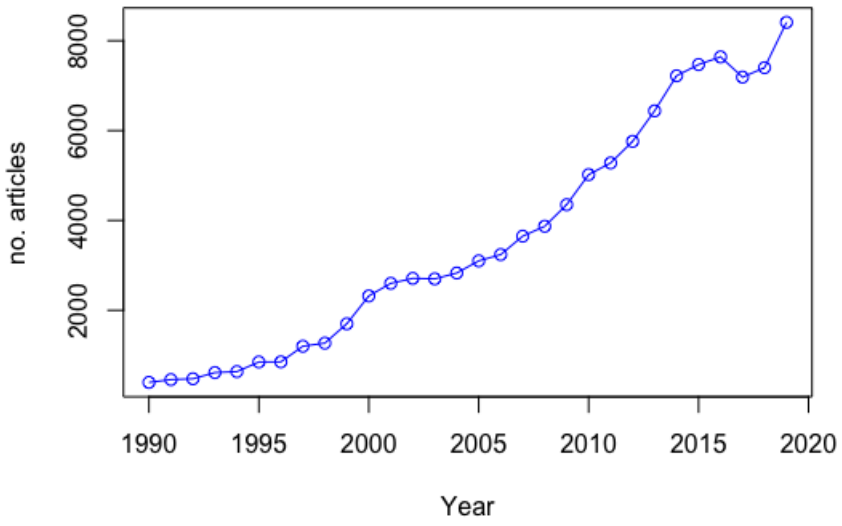
1 Introduction

The balance of forces has shifted in the networked age. People are now public by default and private by effort. Danah Boyd.

We all live in a networked society, where we perform a set of routine activities thanks to our devices and different applications that allow online shopping, communication and social relations, instant access to global information, geolocations, etc. This networking comes with advantages and new paradigms.

On the one hand, the world is undergoing a data revolution, affecting every inch of what we know and facilitating a new tool for a better understanding of everything surrounding us. From the economic point of view, this data production is being recorded, stored and analyzed for the sake of obtaining a competitive advantage for those who own them. However, there is still no general agreement to establish the social benefit of the participants involved.

Figure 1: Studies of privacy-related issues



The information age has a price in terms of privacy. In the words of Hasnat (2018), safety, diversity, pluralism, and democracy are compromised without privacy. In this line, different media point out the great public exhibition to which the new digital age exposes us. This fact, consequently, has been developing privacy concerns in the whole society where privacy and its definition has become a moving target over time, difficult to specify, and an expensive treasure to cherish. Furthermore, this fact is reinforced by the fact that

privacy has been one of the most academically studied topics in recent years and from different academic disciplines. Figure 1 shows the academic studies trend since 1990 in Google Scholar where a remarkable increase can be seen since the 2000s, with a total of 8,410 papers related to privacy studies being published in 2019 compared to 397 in 1990.[1]

This article reviews the notion of privacy over time. The evolution of society and constant technological advance have resulted in a need for a standardization of privacy. The importance in the delimitation between the public and the private domain is of vital importance for making policy recommendations, for the future of institutions and with regard to the regulations currently in force. In concrete, we revise the origin of this notion, "privacy" and how its meaning has evolved over time. Furthermore, we analyse the structure of the markets for personal data, exploring the incentives that organizations may have to monetize their data. We highlight the implications of privacy in the digital economy, and the regulations operating nowadays. This piece of work summarizes the great efforts that have been made in order to protect privacy by institutions and organizations in society. The need for a balance between privacy and security in the markets and for society as a whole, still remains a major challenge.

This article is organized as follows. Section 2 presents "The right to privacy in the digital age". A brief history of the concept of privacy is presented in section 3. Different definitions of privacy are presented in section 4, as we understand it in the 21st century. Section 5 deals with the birth of the markets for personal data and in section 6, we present the implications of privacy as an important threat for the digital economy, and the importance of the digital economy in the world. Section 7 touches on the notions of regulation and protection. Finally, the article concludes with some final reflections on the future of the digital economy and concerns surrounding the paradigm of privacy.

2 The right to privacy in the digital age

On December 18th, 2013, the General Assembly of the United Nations approved the resolution entitled *The right to privacy in the digital age* for all people (United Nations, 2017). This resolution establishes that indiscriminate global surveillance implies a serious violation of human rights, and seeks to reaffirm the fundamental principles adopted in the Universal Declaration of Human Rights of 1948 (article 12), the International Covenant

[1] We searched in Google Scholar the total research papers per year and in which the word "privacy" appears in the title.

on Civil and Political Rights (article 17), and the International Covenant on Economic, Social and Cultural Rights. In particular, this resolution makes it clear that "unlawful or arbitrary surveillance and/or interception of communications, as well as the unlawful or arbitrary collection of personal data, as highly intrusive acts, violate the right to privacy, can interfere with other human rights, including the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association, and may contradict the tenets of a democratic society".

Recognizing privacy as a fundamental right in the digital age highlights the existence of antecedents that denote clear harm and vulnerability for all. Exposure to vulnerability and the possible costs which people can face, due to a misuse of personal information, include:

a) Identity theft: the deliberate use of someone else's identity, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name. The most common cases are Driver's License Identity Theft or Employment Identity Theft. Generally, your personal data is used as your ID.[2]

b) Risk of abuse: personal and professional embarrassment, restricted access to labor markets, and restricted access to best value pricing, (Chaudhry et al. 2015).

c) Privacy breaches: an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. In the last years, there are very striking cases in this context as Yahoo in 2013 with 3 billion stolen data, eBay in May 2014 with 145 million or Uber in 2016 with 57 million.[3] Only in 2019, the most striking cases were: i) Social Media Profiles Data Leak which exposed 4 billion records of personally identifiable information (PII) such as names, email addresses, phone numbers, LinkedIn and Facebook profile information, ii) Orvibo Leaked Database (which runs an IoT platform) with the exposure of more than 2 billion records, and iii) TrueDialog Data Breach (which creates SMS solutions for large and small businesses) exposed over 1 billion records such as full names of recipients, TrueDialog account holders, content of messages, email addresses, phone numbers of recipients and users and much more.[4]

[2]20 types of identity theft and fraud: https://www.experian.com/blogs/ask-experian/20-types-of-identity-theft-and-fraud/.

[3]The biggest data breaches of the 21st century. https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

[4]More information of the Top 12 data breaches of 2019 in:

The attainment of a balance between privacy and security, and how it affects freedom and democracy, is one of the paradigms most studied today.[5]

3 A brief history of Privacy

To understand the problem we are faced with due to a potential violation of our privacy in digital environments, and its effect on freedom and democracy, we must first broach a couple of concepts: the public and the private. This dichotomy is closely linked to freedom. Depending on our conception of what is public or private, and the evaluation that we make of one area or another, we do understand freedom, so we will strive to defend it. And in turn, according to the conception that we have of freedom, we will thus value one and another aspect of our life, and, therefore, our privacy.

On the other hand, it is not strange that the resolution indicates that the non-defense of privacy in the digital age can be contrary to the precepts of a democratic society. In fact, the origins of the first notions of privacy, and of the distinction between private and public, can be found in Ancient Greece. It was with the birth of the *polis* (Greek denomination of city-states), and more specifically with the democracy of Pericles, where these concepts of freedom, democracy and the polarity between private and public spheres were consolidated. An example of this distinction between the public and private can be found in the Greek literature and at the hands of Homer, with his famous work *The Odyssey*.[6] The privacy issue can already be seen in the writings of Socrates and other philosophers too (Moore 1984). For example, it was Aristotle who made the famous distinction between the public sphere corresponding to political activity, and the private sphere of family and domestic life.

Democracy is a basic ingredient in the defense of freedom and thus, privacy. Privacy was born of democracy, and "these delineations could not have been made in the theocracies of the ancient Near East, because in such cultures god-as-ruler permeates everything and no notion of the private is possible", as the author Susan Ford Wiltshire notes.[7]

https://www.securitymagazine.com/articles/91366-the-top-12-data-breaches-of-2019

[5] As an example of these efforts to look for this achievement: the fourth Princeton Fung Global Forum, held in March 2017, in Berlin. https://www.princeton.edu/news/2017/04/13/princeton-fung-global-forum-asks-if-liberty-can-survive-digital-age.

[6] The first explicit opposition between public and private in Greek literature occurs in the Odyssey, pages 8-9.

[7] Ford Wiltshire, S.: Public and private in Vergil's Aeneid, op. cit. "Polarity appeared in the Greek language, however, as early as Homer and it developed in the democratic period of classical Athens. [...]"

In its most fundamental form, privacy was related to the most intimate aspects of the human being. Almost all domestic activities were carried out in front of family and friends, and privacy could mean getting away from society. This makes sense if we think about the origins of humanity, where the first humans were organized in small groups, where the desire for survival did not give rise to the need for privacy. There has always been, as pointed out by Holvast (2007), a kind of conflict between the subjective desire for solitude and seclusion, and the objective to depend on others. Furthermore, this distinction was reflected, as the historian Samantha Burke points out, even in the architecture of the houses, where an attempt was made to balance natural light with the minimum possible exposure (Burke 2000).

On the contrary, later, at the time of the Roman Empire, we found ostentatious houses far from the cities of the rich, which were characterized by wide open spaces that permitted to see and hear what was happening in their interiors. The houses were characterized by having walls where you could hear even the most subtle sounds.

In later centuries, privacy was related to the home, family life and personal correspondence. In fact, from the fourteenth century until the beginning of the nineteenth century, many cases were brought to the court related to listening to or opening and reading personal letters. A very significant example of this in the nineteenth century was the Post Office espionage scandal in 1844, when the Italian nationalist Giuseppe Mazzini accused the British government of opening his letters. Confirmation of his suspicion caused him to file a complaint with the court whose main appeal was based on two key attributes of the letters: that they were private, and that the letters contained secrets. The most important aspect of this event was, without a doubt, and as Kate Lawson points out, that these two claims about the letters helped to create definitions of privacy in personal communications and that the scandal led to the emergence of questions about reasonable expectations of privacy, that are at the same time, Victorian and clearly contemporary (Lawson 2013).

Since the end of the 19th century, the emphasis given to the term of privacy has been directed more towards personal information and its control. For that reason, privacy as we usually understand it dates back no more than 200 years. Even today, despite being a common concept, it is difficult to render a final definition of privacy. And what is more relevant, beyond the global consensus on the importance of privacy and data protection, there is no universal definition of it (Kasneci 2008).

4 What does privacy mean?

Among the first definitions regarding the concept of privacy, as we understand it today, we can cite that expounded by Warren and Brandeis in their famous essay of 1890 (Brandeis and Warren 1890), in which privacy is described "as the right to be let alone". Although, as established by Solove (2005), privacy means different things to different people. One of the most famous and accepted definitions is the one by Westin and Ruebhausen (1967), where privacy is stated as "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others". In this line, Boyd (2010) said that fundamentally "privacy is about having control over how information flows". On the other hand, privacy has been defined as an aspect of dignity, and ultimately, human freedom (Schoeman 1992).

The importance in its definition stands in setting the limits between what is private and what is public. The definition gives rise to the importance of the regulation and protection of personal data.

From a regulatory point of view, the need for a precise definition of this concept is vital. Security in digital markets, what is commonly known as security in information technology or cybersecurity, and its indirect regulation through privacy, has required a greater effort when defining the limits that mark privacy, or, in other words, the boundaries between the self and others, between the private and the public. In this aspect, and in order to create a common path in the definitions, the European Union Agency for Network and Information Security (ENISA) in a recent report highlights the importance of the standardization of concepts such as privacy or cybersecurity. Its importance is maximum when it comes to developing standards that allow for greater international adaptation, transfer of good practices among organizations, promotion of integration and/or interoperability of systems (European Union Agency for Network and Information Security (ENISA) 2019).

5 Markets for personal data

The Internet age is accompanied by a new way of conceiving privacy, adapted to the realities of a global and digital environment. Contrary to what one might think, personal databases of consumers have existed during the twentieth century (Smith 2000). However, due to the progress of information technology and the emergence of the Internet, the scope and reach of those databases have grown considerably. Nowadays, you can store a variety

of very large and rich personal information.

The question is: What kind of information can be stored? From our profiles and demographic data, bank accounts to medical records or employment data. Our web searches, the sites we visited, our likes and dislikes and purchase histories. Our tweets, texts, emails, phone calls and photos as well as coordinates of our real world locations.

According to the World Population statistics, 56.1% of the world's population has internet access, and 81% of the developed world. Therefore, greater access to the Internet generates more personal data and, therefore, greater potential to do business with them.[8] However, we are still not fully aware of the great exposure we have in digital environments. As the World Economic Forum points out in its report Rethinking Personal Data (2012), most people do not have enough knowledge about what can happen with their personal data when using smartphones or the Internet (World Economic Forum 2012). Consequently, this has effects on the digital environment: this leads to fear, uncertainty and the decline of trust and, therefore, to the economic activities developed in digital markets.

In words of the former European Commissioner Meglena Kuneva, "personal data is the new oil of the Internet and the new currency of the digital world". Personal information is power and money, and that is what has led to the birth of a new market ecosystem of organizations that gather, merge, clean, analyze, buy and sell consumer data.

Technology and the migration to an increasingly online life, has led to the massive transmission and disclosure of large amounts of private information by users of different platforms, applications, or any mobile device. These factors have determined the creation of a new market: the personal data market. This ecosystem is complex and decentralized (Olejnik et al. 2014), making it not a unique and unified market.

There are different terms and players in this ecosystem widely used in our daily life such as big data, data mining, data aggregators, data brokers, etc., which play a fundamental role in the digital economy. Big data refers to huge data sets that cannot be as easily stored, processed and accessed as former data collections. In fact, and to put into perspective the amount of data that is generated and processed in the world, "we are reaching the point at which our own capacity to process information rivals that which nature uses to sustain intelligent life" (Hilbert 2012). This implies that we are living through a time in which we are reaching the point of extraordinary orders of magnitude with which mother nature processes information in order to sustain intelligent life. It is through what

[8]Statistics available on: https://www.internetworldstats.com/stats.htm

is known as data mining, that it is possible to identify structures and patterns within the massive amounts of data, such as buying habits, political preferences or credit history. Companies are able to generate important economic profits from knowing this information.

Data is a valuable asset for companies (Moody and Walsh 1999).The monetization of the data, which refers to the use of data to obtain significant economic profits, can be done in two primary ways:

- The first one is internal and focuses on leveraging data to improve operations, productivity and products and services, and also enable ongoing, personalized dialogs with customers.
- The second one is external and involves creating new revenue streams by making data available to customers and partners.[9]

The form of collection and access is simple, and the price for enjoying free online services are important. Indeed, most online services (Google, Facebook etc.) operate by providing a service to users for free, and in return they collect and monetize users personal information (PI). This operational model is inherently economic, as the good being traded and monetized is PI.

However, it is this accessibility, and all subsequent activities that are carried out with personal data, which leads to the emergence of questions related to privacy and security in this ecosystem, having an undeniable relationship with technology. This is where privacy comes in to play and where consumers have an unfavorable position. In short, while there is a market for trading such personal information among companies, the users, who are actually the providers of such information, are not asked to participate at the bargaining table (Spiekermann et al. 2012).

6 Privacy and digital economy

In the digital age, to talk about privacy involves talking about the digital economy. This is due to the fact that the digital economy is financed to a certain extent by organizations with large amounts of unstructured data, some of a personal nature, which facilitate the best adaptation of product offers to individual consumers. For example, search engines

[9]Find out more in: https://sloanreview.mit.edu/article/demystifying-data-monetization/

rely on data from repeated and past searches to improve search results, sellers rely on past purchases and browsing activities to make product recommendations, and social networks rely on selling data to sellers to generate revenues. A very representative and popular example of best adaptation of product offers to consumers and individual tastes is Netflix, a streaming service that allows their members to watch a wide variety of award-winning TV shows, movies, documentaries, etc. On this plaform, the firm's recommendations system strives to help you find a show or movie to enjoy with minimal effort thanks to your interactions on the platform or of other members with similar tastes. Thus, data helps the firm to reinforce customers' experience and to maximize its expected results.[10]

One of the first definitions of the digital economy is found in Tapscott (1996). In this new economy, digital networks and communication infrastructure provide a global platform on which people and organizations create strategies, interact, communicate, collaborate and seek information. Thus, the digital economy refers to an economy based on digital technologies. Digital economics is the discipline that examines whether and how digital technology changes economic activity and explores how standard economic models change (Goldfarb and Tucker 2019).

Table 1: Top 10 most valuable brands in the world in 2018.

Ranking	Brand	Sector	Brand Value 2018 (millions of $)
1	Google	Technology	302,063
2	Apple	Technology	300,595
3	Amazon	Retail	207,594
4	Microsoft	Technology	200,987
5	Tencent	Technology	178,990
6	Facebook	Technology	162,106
7	Visa	Payments	145,611
8	McDonald's	Fast Food	126,044
9	Alibaba	Retail	113,401
10	AT&T	Telecommunication	106,698

Companies have adapted to new technologies and to changes of the 21st century. Table 1 shows the top 10 most valuable brands in the world in 2018 along with the information of

[10] https://help.netflix.com/en/node/100639

the sector they belong to and the value of the brand.[11] The increase in the use of data, the development of artificial intelligence and augmented reality are aspects that have favored brands. As can be seen, eight of the top 10 brands in this ranking are technology-related brands.

Peitz and Waldfogel (2012) study four main topics in the development of the digital economics from an empirical and theoretical point of view: infrastructure; standards and platforms; transformations of traditional selling and new widespread application of tools such as auctions, user-generated contents; and, threats in the new digital environment such as digital piracy and privacy in the digital markets.

The importance of the digital economy in the GDP (Gross Domestic Product), an essential index to measure the economic growth of the countries, emphasizes that it is an undeniable engine of economic growth in the world. According to Accenture Strategy, it is estimated that the digital economy accounts for 20% of GDP in Spain by 2020 (Zamora 2016). However, it is also true that there are difficulties in measuring the real implication of the digital economy as an important aspect for growth in the economy. And this is due to the fact that GDP is essentially a measure of production. While suitable when economies were dominated by the production of physical goods, GDP does not adequately capture the growing share and variety of services and the development of increasingly complex solutions in our 21st-Century digital economy (Wladawsky-Berger 2017).

In particular, the difficulty in measuring it is due to two reasons: i) the traditional forms of measurement of any sector in the GDP as a whole show the need for a new model for the imputation of digital products; and ii) on the other hand, according to Ahmad and Schreyer (2016), many activities, and/or businesses, due to their complexity of control, tracking or measurement will be left out of what is currently computed as GDP of the digital economy.

In addition, the digital economy presents a new paradigm that complicates its measurement as an engine of growth and contribution to GDP, which is the existence of digital spillovers (Oxford Economics 2017). The mechanisms by which this is happening are complex and evolving. Over and above the direct productivity boost that companies enjoy from digital technologies, a more profound chain of indirect benefits also takes place such as the impact spillovers within a firm, to its competitors, and throughout its supply chain.

[11] Information available on https://marketing4ecommerce.net/marcas-mas-valiosas-2018/

7 Regulation and protection of personal data

The Data Privacy Day or Data Protection Day, as it is known in Europe, is an international day that is celebrated every 28th of January, initiated by the European Council and recognized by the United States Senate, Canada and Israel.[12,13,14] The objective of the Data Privacy Day is to increase awareness and promote the best privacy and data protection practices.

The important thing about the existence of this international event is the agreement and intention to walk together towards a law of global privacy. This international celebration offers, as stated in its manifesto, "many opportunities for collaboration between governments, industries, academic institutions, non-profit organizations, privacy professionals and educators" to ensure that the principles of data protection are still in line with current needs.[15]

Nowadays, there are three operational frameworks with respect to privacy, while not mutually exclusive, are sufficiently different from each other. They are mainly represented by China, the United States and Europe. Let us see briefly the legislation and main similarities and differences between them.

7.1 Regulation in EU: GDPR

After 6 years of debate and another 2 years of having been promulgated, on May 25, 2018, the General Data Protection Regulation (GDPR) of the European Union came into force. The new legislation, spelled out before scandals such as Facebook-Cambridge Analytica, is a multidimensional privacy law, robust and with an almost radical strictness with the aim of imposing new rules on the management and the way of sharing personal data.[16]

Among the provisions of the GDPR, the following stand out:

- Data Portability: Require users to continuously give their explicit consent that they accept or not how their information is used, shared and analyzed. In addition, users will have the right to be able to unsubscribe from services without detriment, and they can take their data if they wish, including personal data, encrypted data, metadata, geolocation, and IP among others.

[12] http://www.coe.int/t/dghl/standardsetting/dataprotection/Data_protection_day_en.asp
[13] https://googleblog.blogspot.com/2008/01/celebrating-data-privacy.html
[14] https://www.gov.il/he/departments/topics/international_privacy_day
[15] https://en.wikipedia.org/wiki/Data_Privacy_Day
[16] More information in https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

- Right to be forgotten: The users could demand that the information that a company holds of them be eliminated, as if they had never used the service.

- Right to access and clarity in terms: Users will have the right to request explanations from companies about the decisions that algorithms make about them. In addition, it is demanded that the conditions be unequivocal and specific, so that clauses like "your data will be used to improve our services" will be insufficient.

- New responsibilities that repeal self-regulation: The GDPR expands the responsibility of the companies to the entire chain of data processing, including buyers, suppliers, agents and sub-contractors. In addition, it requires the creation of a Data Protection Officers to maintain and protect information held and be the point of contact with authorities.

- Changes in the protection and filtering of data: It forces the companies to have more "data hygiene" by demanding that they continually justify why they have a piece of information. It also gives the mandate to safeguard the information only in countries that have similar legislation. On the other hand, it obliges companies to report any data breach in less than 72 hours after being identified.

The interesting thing about this regulation is that, in principle, the GDPR only applies to European citizens, but the global nature of the Internet means that almost all services are affected. Furthermore, another of the most important points is that companies should give the opportunity to each user, to be able to download all the data that the company has about him.

This regulation, the GDPR, expands on previous measures of the European Union, such as the privacy shield and data protection directive.[17] Specifically, this expansion goes in two directions:

a) Every time the company collects personal data from an EU citizen, it will need the explicit and informed consent of that person. The importance of this is that it affects companies based outside the EU.

b) The GDPR's penalties are severe enough to get the entire industry's attention; 4% of a company's global turnover or $20 million whichever is larger for any infringements,

[17] Official Website: https://www.privacyshield.gov/welcome

which represents a large increase with respect to the sanctions that were previously applied.

However, the GDPR has not been free of controversies, not only because of the privacy issue, but because of the explosion of costs that it will bring. The new regulation has created a significant demand for privacy professionals, especially in companies that face privacy regulation for the first time (Hughes and Saverice-Rohan 2018). Moreover, according to the study by the IAPP (International Association of Privacy Professionals) in conjunction with EY (Ernst & Young), the Fortune 500 Companies will have to allocate an average of 16 million dollars per corporation to comply with the new regulation. The failure to do so could have the cost of not having access to the European market, mechanisms to share information or services of third parties. At the level of competitiveness, it could delay the development of key technologies such as artificial intelligence, where China is gaining speed due to the gigantic volume of information generated by its inhabitants.

7.2 Regulation in the U.S.

Data protection in the United States is a complex scenario. In the United States, standards and regulations for data processing vary between states, which implies different levels of security and demands depending on where each company operates.

In 2017, data protection in the United States came back to the front pages when Donald Trump signed a law to allow Internet Service Providers (ISP) to sell consumer data without prior consent, invalidating a norm promoted by Obama that dictated otherwise. Although Internet companies such as Facebook and Google already had access to this type of information and collected data from consumers without having to ask for their permission, now ISPs can go further and access the full information on all websites they visit.

The Federal Communications Commission (FCC, an independent agency of the U.S. government) supported the decision to invalidate this part of the Obama era plan to regulate the Internet.[18] This fact was a backward step in the protection of personal data. Defenders of Internet rights, including the former president of the FCC, have been outraged by this law, which is considered to benefit corporations as opposed to Internet users.

[18]More info in https://www.fcc.gov/document/fcc-releases-rules-protect-broadband-consumer-privacy

7.3 Differences between the EU and the United States

The great difference between the United States and the European Union lies in the powers to legislate, which in the case of Europe fall on the European Parliament and in the case of the United States, it is up to the individual states. This fact causes that, while in the EU we have a rule to govern them all, in the US each state has its own data protection legislation.

Furthermore, both policies present different approaches: in the GDPR, European regulators favor an opt-in policy where firms must first obtain consumer consent; on the other hand, American regulators have favored an opt-out policy where concerned consumers can choose to avoid behavioral advertising in order to balance consumer privacy protection. From the users' point of view, opting in is the process by which a user takes an affirmative action to offer their consent. By contrast, opting out is the process by which a user takes action to withdraw their consent. Although they can be seen as different approaches, in reality it is important to keep in mind that wherever there is an opt-in, there needs to be an opt-out, so that users can withdraw their consent at any time. Thus, all in all, recent laws and user demand for greater transparency and control when it comes to personal data, stress the importance of implementing opt-in and opt-out mechanisms.

Following the approval of the GDPR, and pressures from Europe for a tightening of regulations, several states modified their laws or introduced new clauses. However, the big change came in the summer of 2018, when California passed the California Consumer Privacy Act (CCPA), an unprecedented standard in the United States for imposing, for the first time, levels of data protection very similar to those present in the GDPR.[19]

Although the case of California remains unique, it is not the only state that has tightened its regulations in recent times. For example, Arizona has introduced a new notification system in the event of a security breach, while Vermont has passed laws to require greater transparency for those who deal with users' personal information.[20, 21]

Prior to the arrival of the GDPR, the transfer of data between the United States and the European Union was regulated by the Privacy Shield mentioned above, which offered companies a way to self-certify annually to ensure compliance with a series of regulations governing data protection. Nowadays, however, Privacy Shield has been left on the back

[19] More info in https://www.caprivacy.org/

[20] Details available on https://www.azleg.gov/ars/18/00552.htm

[21] Full text available on https://gizmodo.com/vermont-passes-first-of-its-kind-law-to-regulate-data-b-1826359383

boiler due to the obligation to comply with the GDPR. Although it is reviewed annually and has undergone multiple modifications in recent times to adapt to the standards of European regulations, self-certification continues to generate doubts because of its few legal guarantees for practical purposes. Today, Privacy Shield has remained as an extra to provide greater reliability to its customers.[22]

7.4 Regulation in China: between the EU and U.S. approaches

For countries, participation in a globalized economy, international trade, and economic change involves an effort to observe the international standard of privacy and personal data protection. Furthermore, globalization, the exchange of data, and the use of foreign technologies (e.g., Chinese technology), lead countries to commit themselves to privacy and data security. The cost of not committing in this regard could include being excluded from the international game.

China started to develop its data privacy framework much later than the EU and the U.S. Indeed, China's first steps towards protection were due in 2014 while the EU and the U.S. started to develop approaches to data protection in the 1970s (Pernot-Leplay 2020a). China's Cybersecurity Law represents the most significant legal framework for data protection in this country and came into effect on June 1, 2017. This appearance of data privacy regulations in China has occurred under a scenario in which: i) the EU and the U.S. had a large experience on the issue and ii) under the existence of two different approaches in data privacy legislation. Thus, China's regulations share certain similarities with the U.S. approach in several elements but also feature important signs of convergence with EU law (Pernot-Leplay 2020b).

7.4.1 What are the main similarities between China's regulations and EU and the U.S. legislation?

According to Pernot-Leplay (2020a), some of the main similarities and differences are:

i) Data breach notification. It exists in the U.S. but is not as strict as in the EU. In this case, in the U.S. such obligations of notifying personal data breaches exist with a large timeframe for notification, e.g. 30 days or even up to a reasonable time. However, in the EU, data controllers have to notify supervisory authorities of a security breach within 72 hours of becoming aware of it. In China, 2018 Specification

[22]Source: https://es.mailjet.com/blog/news/noticiasproteccion-de-datos-eeuu/

requires tauthorities and data subjects to be informed, but there is no specification on the timescale involved in such notification.

ii) Supervisory authorities. Europe requires an independent and dedicated authority. The U.S. does not provide for a regulatory oversight by an independent data protection authority and China's Cybersecurity Law does not establish an independent authority dedicated to data privacy enforcement either.

iii) Right to be forgotten. The right to erasure that exists in China's Cybersecurity Law is limited to the cases where the network operator has violated laws or agreements between the parties. Therefore, on the one hand the right to deletion is more established in China than in most laws in the U.S. On the other hand, it remains narrower than EU regulations.

iv) Data portability. In the U.S., data portability is required, for example, in California with the California Consumer Privacy Act (CCPA) mentioned above. In the EU, the GDPR recognizes data portability as a data right that spans across sectors. In this case, China follows the EU direction in the 2018 Specification, that grants the data portability right to individuals. However, this right is more limited than in the EU because it only concerns individuals' basic information.

All in all, China's Cybersecurity Law is a significant change for China. The above aforementioned similarities and differences offer specific items that reinforce the idea that China offers more data rights than the U.S. without going as far as the EU. Time will determine the course and development of different laws. The very nature of a globalized economy suggests an international harmonization towards a common path when legislating on privacy and security. This is where standardization of concepts becomes indispensable. Although with some similarities among laws, this fact remains to be seen.

8 Conclusion

The digital economy plays a fundamental role in the world economy and has been the subject of study by many academics and non-academics for some years. Its real impact on the growth of the countries, although it could be incompletely and/or imprecisely measured, points to its growing importance as an engine of economic growth in the upcoming

years. However, as it grows in importance, it also faces numerous threats that put its sustainability and functioning at risk, such as digital piracy, violation, and leakage of private data and cybersecurity.

These threats, which in many cases affect the personal data of millions of users, require some regulation and protection that can establish operating guarantees in the future. Privacy seems to be a moving target, and requires an international effort in order to set a common regulation that can enable the economic development. Standardization turns out to be crucial and requires an ongoing commitment above any political or eventual issue.

Finally, there is a challenge, the need for a balance between privacy and security in our digital age.

References

Ahmad, N. and Schreyer, P. (2016). Measuring GDP in a digitalised economy. *OECD Publishing*.

Boyd, D. (2010). Social network sites as networked publics: Affordances, dynamics, and implications. In *A networked self*, pages 47–66. Routledge.

Brandeis, L. and Warren, S. (1890). The right to privacy. *Harvard law review*, 4(5):193–220.

Burke, S. (2000). *Delos: Investigating the notion of privacy within the ancient Greek house*. PhD thesis, University of Leicester.

Chaudhry, A., Crowcroft, J., Howard, H., Madhavapeddy, A., Mortier, R., Haddadi, H., and McAuley, D. (2015). Personal data: thinking inside the box. In *Proceedings of the fifth decennial Aarhus conference on critical alternatives*, pages 29–32. Aarhus University Press.

European Union Agency for Network and Information Security (ENISA) (2019). Guidance and gaps analysis for european standardisation: Privacy standards in the information security context. *ENISA*.

Goldfarb, A. and Tucker, C. (2019). Digital Economics. *Journal of Economic Literature*, 57(1):3–43.

Hasnat, B. (2018). Big Data: An Institutional Perspective on Opportunities and Challenges. *Journal of Economic Issues*, 52(2):580–588.

Hilbert, M. (2012). How Much Information is There in the information society? *Significance*, 9(4):8–12.

Holvast, J. (2007). History of privacy. In *The History of Information Security*, pages 737–769. Elsevier.

Hughes, T. and Saverice-Rohan, A. (2018). IAPP-EY Annual Privacy Governance Report 2018. *Iapp-Ey*, pages 1–132.

Kasneci, D. (2008). *Data protection law: recent developments*. PhD thesis, Università degli studi di Trieste.

Lawson, K. (2013). Personal privacy, letter mail, and the post office espionage scandal, 1844. BRANCH: Britain, Representation and Nineteenth-Century History. Ed. Dino Franco Felluga. Extension of Romanticism and Victorianism on the Net. Retrieved July 14, 2020 from url https://www.branchcollective.org/.

Moody, D. and Walsh, P. (1999). Measuring The Value Of Information: An Asset Valuation Approach. *Seventh Eur. Conf. Inf. Syst.*, pages 1–17.

Moore, B. (1984). Privacy: Studies in social and cultural history, ME Sharpe. *Inc., Armonk, NY.*

Olejnik, L., Castelluccia, C., and Janc, A. (2014). On the uniqueness of Web browsing history patterns. *Ann. des Telecommun. Telecommun.*, 69(1-2):63–74.

Oxford Economics (2017). Digital Spillover: Measuring the True Impact of the Digital Economy. *A Report by Huawei and Oxford Economics, Oxford, United Kingdom, https://www. oxfordeconomics.com/recentreleases/digital-spillover.*

Peitz, M. and Waldfogel, J. (2012). *The Oxford handbook of the digital economy.* Oxford University Press.

Pernot-Leplay, E. (2020a). China's Approach on Data Privacy Law: A Third Way Between the US and the EU? *Penn State Journal of Law & International Affairs*, 8(1).

Pernot-Leplay, E. (2020b). Data privacy law in China: Comparison with the EU and U.S. approaches. Retrieved July 10, 2020 from url https://pernot-leplay.com/data-privacy-law-china-comparison-europe-usa/.

Schoeman, F. D. (1992). *Privacy and social freedom.* Cambridge University Press.

Smith, R. E. (2000). *Ben Franklin's web site: Privacy and curiosity from Plymouth Rock to the Internet.* Privacy Journal.

Solove, D. J. (2005). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154:477.

Spiekermann, S., Korunovska, J., and Bauer, C. (2012). Psychology of ownership and asset defense: Why people value their personal information beyond privacy. *Available at SSRN 2148886.*

Tapscott, D. (1996). *The digital economy: Promise and peril in the age of networked intelligence*, volume 1. McGraw-Hill New York.

United Nations (2017). The right to privacy in the digital age. thirty-four session. Retrieved July 9, 2020 from url https://documents-dds-ny.un.org/doc/UNDOC/LTD/G17/073/06/PDF/G1707306.pdf?OpenElement.

Westin, A. F. and Ruebhausen, O. M. (1967). *Privacy and freedom*, volume 1. Atheneum New York.

Wladawsky-Berger, I. (2017). Rethinking GDP in the Digital Economy. Retrieved July 9, 2020 from url https://medium.com/mit-initiative-on-the-digital-economy/re-thinking-gdp-in-the-digital-economy-8b309609f20c.

World Economic Forum (2012). Rethinking Personal Data: Strengthening Trust. Retrieved July 16, 2020 from url https://identitywoman.net/wp-content/uploads/WEF2.pdf.

Zamora, A. (2016). Disrupción digital: El efecto multiplicador de la economía digital. Accenture, 1-12. Retrieved July 14, 2020 from url https://circulodeempresarios.org/transformacion-digital/wp-content/uploads/PublicacionesInteres/06.Accenture-Strategy-Digital-Disruption-Growth-Multiplier-Spanish.pdf.