UNIVERSITY OF BRASILIA – UNB

LAW SCHOOL

GRADUATE PROGRAM

MARIANA MOUTINHO FONSECA

THE FEDERAL TRADE COMMISSION AGAINST FACEBOOK:

a law and society approach to consumer privacy and competition policy

Brasilia

2021

MARIANA MOUTINHO FONSECA

THE FEDERAL TRADE COMMISSION AGAINST FACEBOOK:

a law and society approach to consumer privacy and competition policy

Dissertation presented as a partial requirement for the attainment of the Masters' Degree at the Law, State and Constitution Program at University of Brasilia.

Advisor: Professor Alexandre Kehrig Veronese Aguiar, PhD.

Brasilia

2021

MOUTINHO, Mariana.

The Federal Trade Commission against Facebook: a law and society approach to consumer privacy and competition policy. Advisor: Alexandre Kehrig Veronese Aguiar. Brasilia, 2021.

145 pages.

Dissertation (Masters of Law) – University of Brasilia, 2021.

Law School

1. Federal Trade Commission 2. Consumer privacy

3. Competition 4. Digital platforms

APPROVAL SHEET

Mariana Moutinho Fonseca

THE FEDERAL TRADE COMMISSION AGAINST FACEBOOK: a law and society approach to consumer privacy and competition policy.

Dissertation presented as partial requirement to for the attainment of Masters' Degree at Law, State and Constitution Graduate Program at University of Brasilia.

Brasilia/DF, June _____, 2021.

JURY

_____

Professor Alexandre Kehrig Veronese Aguiar, PhD

(Advisor, President)

_____

Professor Ana Frazão Vieira de Mello, PhD

(Internal member, UnB – Faculty of Law)

_____

Professor Rafael Mafei Rabelo Queiroz, PhD

(External member, USP – Faculty of Law)

_____

Márcio Nunes Iorio Aranha Oliveira, PhD

(Substitute)

ACKNOWLEDGEMENTS

Starting and finishing the dissertation in times of pandemic was only possible with the support and affection of a few people. Firstly, I would like to thank my advisor, Professor Alexandre Veronese, who gave encouragement from the first time I spoke with him about applying for the Graduate Program at UnB Law School. Thank you for all the patience and availability, not only in our meetings debating the issues covered in this work, but also for the lessons learnt at classroom.

Thanks to my family, for have always supported me in my career and academics choices, especially during the last months, when I was completely overwhelmed working and writing this work. I am also grateful to my dear Tiago, who was always very caring and patient with me and helped me to stay mentally healthy during this period.

This work was started at University of Connecticut - UConn, where I had the opportunity to start my journey through the American legal system. For the lessons, I want to thank specially to Professor Peter Lindseth, whose class 'Legislation and Regulation' was essential for me to better reflect about the subject of my research, and Professor Kiel Brennan-Marquez, who assisted me in the first steps of this work. Special thanks also to Dave Woods, who helped me a lot during the time I was at UConn. To my friends Felipe Frisoli, Ines Fruechtenicht and Ziyu Wang, who I miss so much and made my time there more memorable. Thank you also to the UConn Library team who was always supportive.

Thanks to my colleagues from the National Telecommunications Agency, in special Isadora Firmino, Lilian Barra, Catarina Gonçalves and Esdras Hoche for providing the conditions for me to study and work simultaneously. Finally, I would like to thanks my friends Fernanda Carvalho, Thales Pereira, Luiza Xavier, Mayhumi Takaki and Danilo Delogo for being good listeners during this journey.

RESUMO

O presente trabalho busca investigar a atuação da Federal Trade Commission (FTC), agência reguladora responsável pela proteção ao consumidor e pela defesa da concorrência nos Estados Unidos, na regulação das plataformas digitais. O modelo de negócio dessas plataformas baseia-se na extração, armazenamento e processamento de quantidades massivas de dados, o que vem despertando preocupações tanto de autoridades governamentais quanto da sociedade civil em matéria de privacidade, tendo em vista a criação e manutenção de um robusto aparato de vigilância privada por estas companhias. Por outro lado, nos últimos anos houve um intenso processo de concentração envolvendo essas plataformas digitais, o que também levanta questões relacionadas à competição e debates sobre as possíveis consequências do acúmulo de uma vasta quantidade de dados nas mãos de poucas companhias. Nesse sentido, autoridades ao redor do mundo vem tentando construir políticas regulatórias que mitiguem os riscos trazidos por essa nova indústria. Em comparação a outras agências, a FTC ocupa uma posição singular por conta do seu duplo mandato e deve se valer dessa vantagem para regular de forma coordenada e mais efetiva plataformas digitais. Esta pesquisa divide-se em três capítulos. No primeiro, apresenta-se o conceito de capitalismo informacional, novo estágio do capitalismo no qual os dados constituem-se como elemento central da produção. Apresentam-se os conceitos de vigilância e de *gatekeeping*, buscando-se demonstrar como eles estão entrelaçados quando se trata de plataformas digitais. No segundo capítulo, busca-se investigar com maior profundidade como tem se dado a atuação da FTC na proteção à privacidade online e à competição em mercados digitais. Apesar de não haver uma lei geral de proteção de dados nos Estados Unidos, a FTC vem atuando de forma crescente nesta matéria e criando uma jurisprudência administrativa sobre o tema. Por outro lado, esta mesma agência autorizou nos últimos anos uma série de aquisições por parte de grandes plataformas digitais. No terceiro e último capítulo, é feito um estudo de caso sobre três investigações empreendidas pela FTC contra o Facebook, dois em matéria de privacidade e um referente a práticas anticompetitivas. Com a análise desses três casos, busca-se compreender quais são as limitações da atuação da agência, bem como de que forma a agência está coordenando suas duas competências na regulação de plataformas digitais.

Palavras-chaves: Federal Trade Commission; privacidade; competição; plataformas digitais.

ABSTRACT

This work seeks to investigate the role of the Federal Trade Commission (FTC), a regulatory agency responsible for consumer protection and promotion of competition in the United States, in the regulation of digital platforms. The business model of digital platforms is based on the extraction, storage, and processing of massive amounts of data, which has been raising concerns from both government authorities and civil society in terms of privacy, considering the creation and maintenance of a robust surveillance apparatus by these companies. On the other hand, in recent years there has been an intense process of market concentration involving these digital platforms, which also raises questions related to competition and debates about the possible consequences of accumulating a vast amount of data in the hands of a few companies. In this sense, authorities around the world have been trying to build regulatory policies that mitigate the risks brought by this new industry. Compared to other agencies, the FTC occupies a unique position given its dual mandate and must take advantage of this position to regulate digital platforms in a coordinated and more effective manner. This research is divided into three chapters. The first chapter presents the concept of informational capitalism, a new stage of capitalism in which data constitutes a central element of production. In sequence, I develop the concepts of surveillance and gatekeeping, seeking to demonstrate how they are intertwined when it comes to digital platforms. The second chapter depicts in greater depth how the FTC has acted in protecting online privacy and competition in digital markets. Although there is no general data protection law in the United States, the FTC has been increasingly active in this matter and creating administrative jurisprudence on the subject. On the other hand, this same agency has authorized in recent years a series of acquisitions by major digital platforms. In the third and last chapter, I undertake a case study on three investigations carried out by the FTC against Facebook, two concerning privacy and one related to anti-competitive practices. With the analysis of these three cases, I seek to understand the limitations of the agency's performance, as well as how the agency is coordinating its two powers in the regulation of digital platforms.

Key words: Federal Trade Commission; privacy; competition; digital platforms.

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

ALJ	Administrative Law Judge
APA	Administrative Procedure Act
API	Application Programming Interface
ARPA	Advanced Research Projects Agency
BC	Bureau of Competition
BCP	Bureau of Consumer Protection
BE	Bureau of Economics
CDA	Communications Decency Act
DOJ	Department of Justice
DPIP	Division of Privacy and Identity Protection
ECJ	European Court of Justice
EU	European Union
DMA	Digital Markets Act
DMCA	Digital Millennium Copyright Act
DSA	Digital Services Act
GAFAM	Google, Amazon, Facebook, Apple and Microsoft
GDPR	General Data Protection Regulation
FCC	Federal Communications Commission
FDA	Food and Drug Administration
FIPPs	Fair Information Practice Principles
FTC	Federal Trade Commission
FTC Act	Federal Trade Commission Act
OECD	Economic Cooperation and Development
OTT	Over-the-top
US	United States
USC	United States Code

SUMMARY

INTRODUCTION

The subject of the present dissertation concerns the role of the Federal Trade Commission (FTC, Commission) in the regulation of online platforms. Particularly, this work aims to analyze, under a law and society perspective, how the FTC, a dual mandate federal administrative agency in the United States, with authority to enforce both competition and consumer protection matters, is formulating policies to regulate the model industry of informational capitalism era, that is, online platforms.

Platforms perform a protagonist role in information society functioning as points of intermediation between distinct but interdependent sets of users, either individuals or firms, who will interact through the service provided.[1] Although social networks and search engines rise as the most prominent examples of platforms, platforms operate in a far more comprehensive range of services, such as e-commerce, accommodation, mobile payments, and transportation. With the growing number of individuals constantly connected, [2] platforms increasingly occupy an important role in users' daily life and the way they consume, work, purchase and even relate with one another.

However, there is a bittersweet character in these transformations, as different segments of society and governments are increasingly concerned with platforms' various services impact on competition, filtering content, misinformation, employment, privacy, and consumer protection. Platforms are particularly known for their reliance upon massive collection and processing of data, a central activity in the data-based economy of contemporary societies. In the information society, data has become the primary source of productivity. However, access to information, differently from other types of assets, is not merely comparable to access to a commodity, as it can also influence the exercise of fundamental rights.[3] For being responsible for a substantial share of commercial services and communications, online platforms have the capacity to control information flows that transit through their services, the accumulation of enormous databases in possession of those companies, along with data pervasive surveillance and manipulation, has raised serious worries about the growing dominance of big technology

[1] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). **An introduction to online platforms and their role in the digital transformation**. Paris: OECD Publishing, 2019, p. 11. Available at <https://doi.org/10.1787/53e5f593-en>. Last access on Jun. 1 2021.

[2] PERRIN, Andrew; ATSKE, Sara. About three-in-ten U.S. adults say they are 'almost constantly' online, **Pew Research Center**, [s.l.], 26 Mar. 2021. Available at <https://www.pewresearch.org/fact-tank/2021/03/26/about-three-in-ten-u-s-adults-say-they-are-almost-constantly-online/>. Last access on Jun 1 2021.

[3] Cf. TAYLOR, Emily. **The Privatization of Human Rights**: Illusions of Consent, Automation and Neutrality, Series Global Commission on Internet Governance Paper Series, Ontario: Center for International Governance Innovation and Chatham House, 2016.

companies, particularly in consumer privacy. On the other hand, online platforms have also posed a challenge to antitrust regulators because traditional antitrust analysis has focused on price evaluation to assess markets. However, as platforms such as Facebook, Google and Amazon offer their services free, they have managed to escape regulatory scrutiny until recently.

In order to address concerns risen by the massive collection of data, public authorities around the globe have made efforts in the last years to regulate information flows and, with that, outline minimum standards for collection and processing personal data as well as recognize a set of rights to those subject to such practices. The most prominent legislation in this realm is the European Union's General Data Protection Regulation (EU's GDPR), which influenced a new generation of data protection laws in countries such as Brazil (General Law on Personal Data Protection, Statute n. 13.709/2018), India (Personal Data Protection Bill, 2019), South Africa (Protection of Personal Information Act, 2019), or amendments to existing legislation around the globe, as Australia (Privacy Act, amended in 2018) and Japan (Act on Protection of Personal Information, amended in 2017). Regulatory authorities in Europe have also been concerned about the effects of the emergence of big online platforms to economic relationship, what led the European Commission to submit in December 2020 the Digital Services Act (DSA) and the Digital Markets Act (DMA) proposals, which have been saluted as a further step towards a tougher oversight of the technology industry.[4] Similarly, after years of unencumbered growth, China's tech giants such as Alibaba, Tencent, Baidu are also currently in the crosshairs of Chinese regulators which have drafted rules against monopolistic practices, data protection, and capital requirements for technology firms.[5]

In the United States (US), the FTC emerges as probably the most relevant regulatory authority in the debate about the regulation of online platforms services. The Commission has a dualistic mission of protecting American consumers and promoting competition, but differently from other agencies, it does not target any specific industries, such as the Federal Communications Commission (FCC) or the Food and Drugs Administration (FDA) do. The broad mandate granted to the FTC to regulate unfair and deceptive acts or practices depicted in

[4] SATARIANO, Adam. Big fines and strict rules unveiled against 'Big Tech' in Europe. **New York Times**, New York, Dec. 15 2020. Available at <https://www.nytimes.com/2020/12/15/technology/big-tech-regulation-europe.html>. Last access on May 30, 2021.

[5] KHARPAL, Arjun. China's move to regulate its tech giants is part of its bigger push to become a tech 'superpower'. **CNBC,** [s.l.], (Jan 12, 2021), Available at <https://www.cnbc.com/2021/01/11/chinas-tech-regulation-part-of-bigger-push-to-become-a-superpower-.html>. Last access on May 30, 2021.

Section 5 of the Federal Trade Commission Act (FTC Act)[6] has permitted the Commission to ascend to protagonist role in US privacy regulation scene, performing a role of American data protection authority. Indeed, the FTC settlements in privacy matters have constituted one of the strongest sources of privacy law in the country,[7] although usually overlooked by foreign scholars. The FTC also has played an important role in its original competence to enhance competition in American markets through the combat of unfair methods of competition depicted in the FTC Act and the analysis of mergers and acquisitions under the Clayton Act. Despite the existence of considerable literature analyzing both competences of the FTC, there have been few works analyzing the interactions of regulatory policies both in privacy and competition realms, particularly concerning the FTC's decisions targeting online platforms.

This work aims to bring a modest contribution to this field. This investigation is relevant because both competition and privacy concerns seem to derive from the massive accumulation of data online platforms markets. Comprehensive data harvest has its roots in the construction by those online platforms of a sophisticated and ubiquitous private surveillance apparatus, which has consequences to the exercise of privacy rights and implications on consumer protection, self-autonomy, and social inequalities. On the other hand, the accumulation of data also seems to have an impact on competition due to the existence of strong network effects on digital markets. Fresh startups from the Silicon Valley born in a highly innovative and competitive market turned into technology conglomerates, raising questions about the legality of their commercial practices and the possible consequences of obtaining valuable datasets. Through the analysis of the recent FTC complaints, but particularly focusing on the three cases filed against Facebook, I also intend to investigate the limitations of the enforcement-based model and suggest some possible improvements. An in-depth analysis of the Facebook cases is particularly interesting to understand how consumer privacy and competition regulation intertwine because it was the first time the Commission challenged a big technology company in both realms. As our focus, therefore, will remain in the role of the FTC, which already possesses a rich body of decisions and guidance documentation, this work does not intend to cover American state law. Nor it aims to bring other debates involving online platforms, such as regulation of content or intellectual property, despite the relevance of studies in these fields.

[6] UNITED STATES. UNITED STATES CODE (USC). Title 15, Ch. 2, §§41-58 Federal Trade Commission Act (FTC Act). Available at https://www.ftc.gov/sites/default/files/documents/statutes/federal-trade-commission-act/ftc_act_incorporatingus_safe_web_act.pdf.

[7] SOLOVE, Daniel J.; HARTZOG, Woodrow. The FTC and the new common law of privacy, **Columbia Law Review**, v. 114, n. 3, p. 583–676, 2014.

This work is divided into three chapters. In the first chapter, I will contextualize the research problem, bringing the concept of informational capitalism developed by communication theorist Manuel Castells and the main characteristics of the new technological paradigm (section 1.1). Then, I will give a brief explanation of the concept of platform and its business model (section 1.2) and present the two ways through which platforms exercise power in the networks, that is, gatekeeping and surveillance. At the end of the chapter, I will demonstrate how they are intertwined. (section 1.3).

The second chapter begins with an investigation about how legal constructions in the United States in consumer privacy and antitrust realms have influenced regulatory policies in the last years and the consequences they brought to the development of platform markets (section 2.1). Then I will provide a short explanation about some foundational aspects of American Administrative Law, particularly the sources of agency action depicted in the Administrative Procedure Act (APA) (section 2.2). Finally, I will properly address the role of the FTC in regulating online platforms (section 2.3). Firstly, through the construction of its privacy authority through the enforcement action against unfair and deceptive acts or practices (subsection 2.3.1) and, secondly, the Commission's role in enforcing antitrust laws and challenging anticompetitive mergers and acquisitions that could harm consumers (subsection 2.4.2).

The third and last chapter brings a case study about the FTC action against Facebook. As will be seen, in a ten years period the Commission filed three complaints targeting Facebook, the two firsts related to privacy violations (subsections 3.2.1 and 3.2.2), and the third one regarding anticompetitive practices (subsection 3.2.3). These cases were chosen because they constitute the first set of cases in the FTC history in which a big tech is challenged in both privacy and antitrust realms. Through the analysis of the three complaints, I expect to verify how the Commission in a broad scenario is dealing with the harms associated with platforms' practices.

CHAPTER 1 PLATFORMS IN THE AGE OF INFORMATIONAL CAPITALISM: BETWEEN SURVEILLANCE AND GATEKEEPING

1.1 FROM ATOMS TO BITS, FROM PLANTS TO CODE: THE TRANSITION FROM INDUSTRIAL TO INFORMATION SOCIETY AND THE NEW TECHNOLOGICAL PARADIGM

The last decades of the twentieth century and the first decades of the twentieth-first century were marked by an accelerated transition from a traditional industrial society, driven by economies of scale, automatization, and production of goods, to a new mode of development, founded on information technologies. Beginning in the 1970s, the diffusion of microelectronics, with the invention of the first commercially produced microprocessor Intel 4004, and of microcomputers, with the launch of the Apple and the personal computer by IBM years later, as well as the construction of a communication network by the US Defense Department's Advanced Research Projects Agency (ARPA) that would become the Internet lately, not only brought more comfort for people's daily lives but would also remodel production, labor, and even demographics. Although the ideas of "information" and "knowledge" have been present in the capitalist mode of production as a key need to the organization of large-scale production and exploitation of labor[8] and data have long been used to enhance economic processes, in the current century information not only became considerably cheaper but there was also a significant expansion in its handling. However, it is neither the volume of information circulating nor the information-related positions in the market that should characterize an information society, as the growing indispensability of a phenomenon for itself is not capable to identify a new social order. Not even the sole fact that information has been stored, transmitted, or sent through in electronic media, although technological advances have played an important part.

Indeed, as highlighted by Frank Webster, despite the importance of technological advances for this phenomenon, the idea of an information society refers to a systemic change, rather than a sheer expansion of information circulating in the world.[9] There are many ways and strands to define what constitutes an information society, although all theorists concerned with the subject consider that there is something special about information in the contemporary

[8] AMPUJA, Marko; KOIVISTO, Juha. From 'Post-Industrial' to 'Network Society' and Beyond: The Political Conjunctures and Current Crisis of Information Society Theory. **TripleC: Communication, Capitalism & Critique**, v. 12, n. 2, p. 447–463, 2014.

[9] WEBSTER, Frank. **Theories of the Information Society**. 3 ed. New York: Routledge, 2006, p. 22-23. Webster claims that "we must not confuse the indispensability of a phenomenon with the capacity for it to define a social order".

world.[10] For instance, in 1976, Daniel Bell argued that it was underway a transition from an industrial to a post-industrial society.[11] In post-industrial societies, information acquires more importance than raw muscle, power, or energy, and the central person is the professional, that is, the individual that has a good level of education and technical skills necessary to perform tasks that require some degree of intellectual sophistication.[12] Bell claims that "theoretical knowledge", acquired through education, and not wealth or property, is what would provide access to income and privilege.[13] The focus of post-industrial societies was on the provision of services rather than industrialized goods, more specifically professional and technical services.

Similarly to Bell, Manuel Castells also considers that industrialism was superseded by a new step of the capitalist mode of production called “informationalism”, a mode of development[14] in which “the source of productivity lies in the technology of generation, information processing, and symbol communication”.[15] Information has been an essential factor in previous stages of capitalism, but differently from them, informationalism has its roots in technological development, the accumulation of knowledge, and higher levels of information processing.[16] Besides, informationalism distinguishes by its global scale and its dominant functions and processes be organized around networks.[17] In this sense, whereas Bell considers the states as the main inducers of the transition from industrialism to informationalism, Castells sees private actors operating in networks horizontally structured as the driving force of such movement.[18] Thus, as will be later developed, power in the network society will not lie mainly

[10] Ibid.
[11] Daniel Bell classified societies in preindustrial, industrial, and post-industrial. Preindustrial societies were focused on extractive industries, like mining, agriculture, fishing, which demanded a strong and abundant workforce. Industrial societies are characterized by the massive production of goods, and energy is the driving force of production. BELL, Daniel. The coming of the post-industrial society. **Educational Forum**, v. 40, n. 4, p. 575–579, 1976.
[12] Ibid, p. 576.
[13] As we will see in the next sections, the notion of property and production of wealth will be also deeply affected by the centrality of information in the shift from an industrial society to an informational one.
[14] According to Castells, "mode of development" consists of “the technological arrangements through which labor works on the matter to generate the product, ultimately determining the level and quality of surplus. Each mode of development is defined by the element that is fundamental in fostering productivity in the production process. Thus, in the agrarian mode of development, the source of increasing surplus results from quantitative increases of labor and natural resources (particularly land) in the production process, as well as from the natural endowment of these resources. In the industrial mode of development, the main source of productivity lies in the introduction of new energy sources, and in the ability to decentralize the use of energy throughout the production and circulation processes”. CASTELLS, Manuel. **The Information Age, vol. 1: The Rise of the Network Society**. 2 ed. Oxford: Blackwell Publishing, 2010, p. 16.
[15] Ibid, p. 17.
[16] Id.
[17] Ibid, p. 500-502.
[18] AMPUJA; KOIVISTO, op. cit.

in the hands of public officials or traditional capitalists, but in the hands of those who have control of communication networks.[19]

In order to explain the technical, organizational, and managerial innovations brought this new mode of development, Castells develops what would be the features of the information technology paradigm. The idea of technological paradigm "helps to organize the essence of

current technological transformation as it interacts with economy and society".[20] He enumerates five features that constitute the information technology paradigm. First, the fact that these are technologies to act on information. Second, the pervasiveness effects of new technologies in individual and collective processes. Third, the network logic of relationships built in the information society. Fourth, the flexibility of the new paradigm. Fifth, the ongoing phenomenon of digital convergence. In the next paragraphs, I will provide a short explanation of these features.

The first feature, *technologies that act on information*, refers to the fact that, whereas in industrial societies energy sources functioned as raw material, in informational ones data is the main source of production. "The world's most valuable resource is no longer oil, but data"[21] is a phrase often seen in the media referring to how data has become a commodity of the lucrative digital industry. Similar to oil, information can be extracted, refined as used for multiple purposes.[22] Property of information (intangible resources) is becoming more valuable than the property of oil and other material goods, but information has played an essential role in the construction of networks and relationships, even when is not associated with commercial trades. The right to freedom of speech, for instance, has been essential to guarantee the free exchange of information in society and allow people to form an opinion in different realms – the notion of 'marketplace of ideas' carved by Justice Oliver Wendel Holmes in his famous dissent in *Abrams v. United States*[23] – as well as to hold governments and other institutions accountable for their actions, insofar as the more knowledge people have, the more means they have to supervise public officials and private actors that perform some function of collective interest, such as companies, churches, and non-governmental organizations.

---

[19] CASTELLS, Manuel. **Communication Power**. 1 ed., New York: Oxford University Press, 2009.
[20] CASTELLS, op. cit., 2010, p. 70.
[21] Cf., for instance, THE WORLD'S most valuable resource is no longer oil, but data. **The Economist** (May 6th, 2017). Available at https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data
[22] SRNICEK, Nick. **Platform Capitalism**. Cambridge, UK: Polity Press, 2017, p. 75.
[23] UNITED STATES. Supreme Court. Abrams v. United States, 250 US 616. Nov. 10, 1919. Available at < https://supreme.justia.com/cases/federal/us/250/616/>. Last access on Aug. 5, 2020.

In the very early days of the Internet, there was an optimistic feeling that information flows would transit boundlessly, without any kind of state regulation and risk of censorship, leading to empowerment of individual's voices and bringing more equality of speech to the public arena.[24] With information traveling freely on cyberspace, the problem of scarcity seems to be solved: if you want a book, a music album, but cannot afford it, someone will make a copy for you.[25] However, in private markets, information is seen as a commodity, subject to the law of economics, rather than public good.[26] Thus, it turned necessary to give incentives to creators and inventors to produce more information - intellectual property rights - that permit them to profit from their creations and prevent the free-rider actions.[27] Such construction, tough, becomes more complex in the information age, as digitalization leads not only to a detachment between information and physical good – just as wine without a bottle.[28] In this scenario, where transmission and reproducibility of information faster and less costly, enforcement of intellectual property rights became a challenge, leading to a movement to expand such rights. This shift towards privatization of technological barriers[29] and anti-circumvention laws[30] led to what scholars called a "second enclosure movement", as a reference to the privatization of common lands in England from the fifteenth century to the nineteenth century.[31]

As the second feature, Castells points out the "*pervasiveness of effects of new technologies*": as dealing with information is inherent to all human activities, the new technological medium based on information processing utterly reshapes individual and collective processes.[32] In this sense, Cohen considers that the movement from an industrial economy to an informational one is redesigning the basic factors of production of capitalist

[24] JOHNSON, David R.; POST. David, Law, and Borders : The Rise of Law in Cyberspace, **Stanford Law Review**, v. 48, n. 5, p. 1367–1402, 1996. BARLOW, J. P. A Declaration of the Independence of Cyberspace. **Electronic Frontier Foundation**. [s.l.], Feb. 8 1996. Available at: <https://www.eff.org/cyberspace-independence>. Last access on Jun. 17 2020.

[25] MURRAY, Andrew D., op. cit., p. 13.

[26] BOYLE, James. A Theory of Law and Information: copyright, spleens, blackmail, and insider trading. **California Law Review**, v. 80, n. 6, p. 1413–1540, 1992, p. 1438-1439.

[27] Id.

[28] BARLOW, John Perry. Selling Wine Without Bottles : The Economy of Mind on the Global Net. **Electronic Frontier Foundation**. [s.l.], 1994. Available at: https://www.eff.org/pages/selling-wine-without-bottles-economy-mind-global-net. Last access Jun 17, 2020.

[29] For instance, the digital rights management, which consists of the use of technology to control access and limit copying of copyrighted works and proprietary software. It may involve codes to restrict or prevent users from editing, saving, forwarding, sharing, or printing, as well as to set a limited number of accesses or an expiry date.

[30] Cf., for instance, the Digital Millennium Copyright Act of 1998 enacted by the United States Congress, and the Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases, 1996 O.J. (L 77) 20, available at http://europa.eu.int/ISPO/infosoc/legreg/ docs/969ec.html

[31] BOYLE, James. The second enclosure movement and the construction of the public domain. **Law and Contemporary Problems**, v. 66, n. 33, p. 33–74, 2003, p. 37.

[32] CASTELLS, op. cit., 2010, p. 70.

order: money, land, and labor.[33] In the digital era, the development of instantaneous communications networks permitted an acceleration of trades in national and global markets. In 2019, the global electronic commerce retail market was estimated at $25.038 trillion,[34] and $441.1 billion purchase transactions were made using credit cards worldwide.[35] The increase of online commerce and cashless payment platforms lead to demonetization, with blockchain technologies nowadays being used to authenticate transactions and transfer money through countries. Money has become detached from real-world activities, as a consequence of the growing complexity of financial transactions. Similarly, there is a growing separation between interests in real property and the material world.[36] For instance, when a mortgage loan changes hands, it is important to preserve the chain of title and protect the current mortgage holder in case of failure to repay the debt. As mortgages subject to securitization change ownership fast, it was created the Mortgage Electronic Recordation System (MERS), which separates the promissory note (the title creating the borrower's obligation to repay the debt) from the mortgage instrument (the document creating an interest in real property as security for the loan).[37] However, MERS failed in keeping records of the chains of titles of securitized loans and the correspondent real property, which also contributed to the 2008 market crash.[38] Although there was an expectation that technology would make transactions like these more transparent, that has not happened, as algorithm-driven systems add layers and layers of opacity to these transactions.[39] The digital economy also promotes changes in the division of labor, with work divided between *self-programmable labor* – undertaken by professionals with abilities to gather relevant information, associate it to knowledge and apply it in processes of production - and *generic labor* – consistent of less qualified tasks, machine replaceable or transferable to areas with lower production costs.[40] In information economy, generic labor is associated with practices based on temporary employment and freelance production. Global technology industries, such as Amazon and Uber, argue that such practices promote exceptional benefits

[33] COHEN, Julie E., op. cit., 2019, p. 29.
[34] LIPSMAN, Andrew. Global Ecommerce 2019: e-commerce continues strong gains amid global economic uncertainty. **Emarketer**, [s.l.], Jun. 27 2019. Available at <https://www.emarketer.com/content/global-ecommerce-2019>. Last access Jun 19, 2020.
[35] RUDDEN, Jennifer. Number of card transactions worldwide in 2019, by brand. **Statista,** [s.l.], Aug. 7 2020. Available at <https://www.statista.com/statistics/261327/number-of-per-card-credit-card-transactions-worldwide-by-brand-as-of-2011/>. Last access Jun 19, 2020.
[36] Cohen, op. cit, p.41.
[37] Id.
[38] Ibid. p. 42.
[39] PASQUALE, Frank. **The black box society:** The secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.
[40] CASTELLS, op. cit., 2009, p. 30.

for the economy and workers, as it improves fairer competition in the labor market due to its lower-cost entry, prevents unemployment, and allows flexible working hours.[41] However, other narratives about the gig economy are emerging: this new class of intermittent workers that offers its services in a needed-basis way are invisible, left to precariousness due to insecure and poorly paid conditions.[42]

The third feature of the new technological paradigm relates to the *networking logic of the relationships* constructed in the information society.[43] Networks are open structures of communications composed of interconnected nodes and built around settled goals, interests, and values. What constitutes a node will vary depending on the network one is analyzing (Internet users, stock exchange markets, governmental actors, academic researchers, and so forth).[44] Networks can expand without limits through the integration of new nodes, so they are highly dynamic and innovative.[45] Along with the emergence of new communication technologies, these horizontal digital networks acquire a central role in comparison to vertical and hierarchical structures of society, which historically have been the focus of research on organizational studies.[46] Because of their horizontality, it is challenging task to have effective control of a network. Notwithstanding, some of the nodes in networks exert more influence than others due to their capacity to gather, transmit, and processing information relevant to the network's goals, functioning as *gatekeepers*. Emily Laidlaw explains that gatekeepers are "non-state actors with the capacity to alter the behavior of others in circumstances where the state has limited capacity to do same".[47] Laidlaw identifies two basic roles of gatekeepers: to control who has access to information and to what kind of information, and to act as intermediaries and facilitators.[48] Gatekeepers, though, may vary in their capacity to influence. Andrew Murray explains that nodes in a network have different regulatory weights, and may exert different

[41] PASQUALE, Frank, Two narratives of platform capitalism, **Yale Law & Policy Review**, v. 35, p. 309–320, 2016.
[42] Ibid.
[43] CASTELLS, op. cit., 2010, p. 70.
[44] Id., p. 501.
[45] Ibid.
[46] CASTELLS, op. cit., 2009.
[47] Emily Laidlaw calls attention to the role performed by the so-called "Internet Information Gatekeepers", who have the power to facilitate or limit democratic discourse on cyberspace. Internet Information Gatekeepers may be classified as micro-gatekeeper, authority gatekeeper, or macro-gatekeeper depending on i) whether the information is meaningful to democratic debate; and ii) their reach and structure. LAIDLAW, Emily, A Framework for Identifying Internet Information Gatekeepers, **International Review of Law, Computers & Technology**, v. 24, n. 3, p. 1–16, 2010, p. 2.
[48] Id.

levels of gravitational pull.[49] Thus, the more weight they have, the more they are capable to impose their rules through the online environment.[50]

The fourth feature consists of the *flexibility of the new technological paradigm*, in which processes are reversible and organizations or institutions can be rearranged.[51] Information and communication technologies offer a distinctive level of configuration, favoring the dynamism of networks, particularly on the Internet-based services. Differently from architecture in the real world, in which costs of changing can be high, in the online environment, the code is plastic,[52] which means that networks can be constantly subject to reconfigurations, self-improvements, according to circumstances and demands. Nonetheless, Lawrence Lessig argues that the potential plasticity of code does not imply more liberty. Just as constitutions are built over time and not merely found, there is no reason to believe that structures of freedom in cyberspace will simply rise.[53] How would be possible to regulate the online environment in this context? Lessig considers that, as it would be difficult to governments to regulate behavior in cyberspace, direct regulation by law in cyberspace probably would not prevail. However, indirect regulation by law, through which legal norms proscribe commands to be executed by the code and are directed to code writers, would have the effect to oblige platforms to regulate in order to achieve certain goals. [54] Thus, given cyberspace's architecture, it would be more efficient for governments to regulate the architecture of the Internet itself, although the regulation of code indeed could be challenging.[55] Legal institutions offer points of entry for economic and political power and, because of that, encompassing multiple parties disputes about is the role of private and state actors, what can be considered as actual or potential harm.[56] On the other hand, Castells argues that, although flexibility can be a liberating force, it can also transmute in a repressive tendency if those with the capacity to write the rules (or code) are the same

[49] MURRAY, Andrew D. Nodes, and gravity in vitual space **International Journal of the Study of Legislation**, v. 5, n. 1, p. 195–221, 2001.
[50] It should be noted, however, that Murray considers, based on his network communitarism theory, that for a regulatory settlement to be considered effective the individual nodes of the network must accept the settlement. Ibid, p. 219.
[51] CASTELLS, op. cit., 2010, p. 71.
[52] LESSIG, Lawrence. **Code and Other Laws of Cyberspace ver. 2.0**. New York: Basic Books, 2006.
[53] Ibid, p. 4.
[54] Id.
[55] Lessig compares the forces that restrain one's behavior in the 'real world' with those that act on the same individual in cyberspace. In the real world, a person may have her behavior shaped by the law, social norms, architecture, and the market, whereas in cyberspace a person's behavior is shaped by the law, social norms, and the code/architecture. In cyberspace, regulation by code is more effective than regulation by law. Thus, Lessig proposes that government should increase regulability in cyberspace through the regulation of code by the law. LESSIG, op. cit., p. 61-62.
[56] COHEN, Julie E., op. cit., 2019, p. 3.

constituted powers.[57] Technologies are not necessarily neutral, stakeholders can shape their development and build structures that reproduce economic and political power, or protect values that are fundamental to society.[58] As will be seen in chapter 2, narratives about innovation and deregulation had had a meaningful impact on the legal debate.

Finally, the fifth feature consists of the growing access to the Internet in the last decades that lead to a move towards digital convergence, making possible the exchange of different media content – voice, data, and video - through a single carrier. Until the end of the twentieth century, different modes of communication – telephony, broadcasting – were constructed to carry out information in separate ways, each one with its structures and corresponding regulatory frameworks.[59] This started changing with the digital convergence movement, leveraged by technological advances on processing capacity as well as by the policy decision to standardize protocols to make data interchanges more feasible.[60] These two factors contributed to the massive expansion of the Internet in the 1990s with the World Wide Web protocol. In the following years, advances in wireless and broadband transmissions in the following, it allows a growing demand for diversification of content to be created, shared, and sent online. Such technological transformation enables a rich environment within which individuals performed a role of active users rather than passive consumers of content, a different kind of relationship, thus, that they traditionally have with mass communication media until then, as merely receptors.[61]

Going live stream on Instagram, posting on Reddit, commenting on a YouTube video, having a chat with peers around the globe through WhatsApp, are all examples of how technology has made possible to individuals to send instantaneously different kinds of content

---

[57] CASTELLS, op. cit., 2010, p. 71.

[58] COHEN, Julie E., op. cit., 2019, p. 5 ("Code will be a central tool in this analysis. It will present the greatest threat to both liberal and libertarian ideals, as well as their greatest promise. We can build, or architect or code cyberspace to protect values that we believe are fundamental*"*).

[59] BLACKMAN, Colin R. Convergence between telecommunications and other media How should regulation adapt?. **Telecommunications Policy**, v. 22, n. 3, p. 163–170, 1998, p. 164.

[60] Mueller affirms that increase of microprocessors capability followed by lower costs of productions (Moore's law), together with the adoption, at first, of protocols such as ISDN and Ethernet, and later on, TCP/IP, which became "the protocol of convergence". "*The Internet protocol suite (TCP/IP) was designed to support internetworking. This means that it permits the interconnection of multiple networks that use different hardware and communication conventions. (...) The basic technology of TCP/IP has survived almost two decades of exponential growth. During the past three years, TCP/IP has become the "protocol of convergence" for many companies and services. Internet telephony, and the streaming of video and audio on the Internet, is now commonplace, although the quality of service offered rarely matches that offered by networks based on more traditional standards*". MUELLER, Milton. Digital Convergence and its Consequences. **Javanost - The Public**, v. 6, n. 3, p. 11–27, 1999.

[61] BENKLER, Yochai, From Consumers to Users : Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access, **Federal Communications Law Journal**, v. 52, n. 3, p. 561–579, 2000 p. 562.

either to one person or to a global audience, and also receive information through infinite different sources, rather than just from a very restricted group of media passively. Castells defines this new relationship as "mass self-communication" this new Internet-based mode of communication through which individuals build multimodal horizontal networks based on their interests, ideas, and desires.[62] However, those networks should not be taken for granted. Yochai Benkler warns that the shift from consumer to user can only occur through the means of policy agenda focused on the identification of the necessary resources to exchange information through the network and on guaranteeing access equally and ubiquitously to all users.[63] The rearrangement of communications infrastructure carried out by digital convergence, thus, emerges as a crucial factor for the massive production, transmission of data that characterizes modern social, economic, and cultural structures of the information society.

These five features taken together are useful to set up the scenario to understand better the new economy that emerged at the end of the twentieth century and blasted off in the last two decades. The networked construction of the communication structures and the movement towards digital convergence result in a massive amount of information, in different media, exchanged through the Internet. Thus, those actors who function as points of control and organization of information flows have the capacity to, through modification of the architecture of the Internet, intervene and reshape a wide range of relationships, reforming commerce, labor, culture, and even political process. In this sense, the trends brought by informationalism associated with the capitalist mode of production has high-tech companies, particularly Internet-based platforms, as its model industry. Therefore, the next section will explore in-depth how they emerged as the driving force of informational capitalism and how their business models function.

1.2 THE PLATFORM AS THE TOUCHSTONE AGENT OF INFORMATIONAL CAPITALISM

Before continuing this analysis, is important to justify my choice for the usage of the expression 'informational capitalism' among other possibilities, as there have been a different number of expressions to describe the phenomenon that merges information society features and capitalism. Manuel Castells, and Julie Cohen afterward, depict the fusion of informationalism as mode of development and capitalism as mode of production as

[62] CASTELLS, op. cit., 2009, p. 63.
[63] BENKLER, op. cit., p. 562.

'informational capitalism'.[64] Other authors, such as Shoshana Zuboff, names ‘surveillance capitalism’ the new mode of production in which the commodification of personal data and the development of highly elaborated practices of information extraction and processing driven to profit is achieved through systematic private surveillance of users.[65] Ivan Manokha also describes this idea of surveillance as a central feature of the economy.[66] On the other hand, both Nick Srnicek[67] and Frank Pasquale[68] adopt the expression 'platform capitalism', focusing on major technology companies as the main economic actors in the new capitalist mode of production. These expressions are not exactly fungible. Nonetheless, all those theoretical frameworks have something in common. At their core, the idea of ownership of data and of the means to process it is crucial for the distribution of power in the network society. In this new economic order, supervision is build up towards more efficient processes to guarantee profit. Capitalists principles such as profit maximization and market competition are still valid here, but they operate in a new logic of accumulation, characterized by methods and processes to extract information of potential consumers, with that, as will be seen in more detail through this chapter, provide more customized services and products that they will be more tended to purchase.[69]

In this dissertation, I consider that it makes more sense to adopt the terminology 'informational capitalism'. Firstly, because the authors that adopted 'informational capitalism' as terminology to explain this series of social, economic, technical, and cultural phenomena follow a law and society approach, which means that they aim to understand law through their structures, social contexts, and practical application of those rules, what I will attempt to follow while analyzing the Federal Trade Commission regulation. Secondly, the preferential use of 'informational capitalism' over other terminologies relies on the belief that the changes depicted in the last section, which constitutes the foundation of informationalism as the new mode of development, were essential for the construction of the prevalent business model in this new phase of capitalism. Despite the crosscutting character of transformations and innovations through which companies have been passing in the information age, traditional business models are not the best suited to this job, leveraging the emergence of a new type of firm: the digital

[64] CASTELLS, op. cit., 2010; COHEN, Julie E., op. cit., 2019**.**
[65] ZUBOFF, Shoshana. **The Age of Surveillance Capitalism:** the fight for a human future at the new frontier of power. 1 ed., New York: PublicAffairs, 2019.
[66] MANOKHA, Ivan. Surveillance: The DNA of platform capital — The case of Cambridge Analytica put into perspective. **Theory and Event**, v. 21, n. 4, p. 891–913, 2018.
[67]SRNICEK, Nick. op. cit.
[68] PASQUALE, op. cit, 2016.
[69] ZUBOFF, op. cit., p. 50; COHEN, op. cit., p. 80-85.

platform[70]. Platforms rest in the very heart of informational capitalism. When one thinks about the digital economy, probably the first companies that will come to mind will be Google, Amazon, Facebook, Apple, and Microsoft ("GAFAM"). This is not without reason. These companies, which have pervasively occupied spaces in the daily life of individuals, are in the world's top 10 companies by market value in 2019, leading to the conclusion that this business model has very successful and profitable.[71] However, the concept of platform encompasses a wide array of businesses.

So, what defines a platform? In a very broad and traditional definition, it can be described as a foundation upon which other processes are developed. Tarleton Gillespie recalls that, in the past, the word platform could acquire four meanings.[72] The first, a computational meaning, as an infrastructure that is used to give support to other applications, like a computer hardware or an operational system. The second, an architectural definition, as a surface where people or things could stand. The third, a figurative connotation, as a synonym to 'ground', 'foundation', 'basis of an action'. Finally, a political meaning, referring to the subjects that grounded a politician or a party's speech.[73] Despite criticism that the term platform is too broad,[74] more recently, the word platform has been used to refer to a type of business model that facilitates interaction and exchanges among users through the creation or connection of networks with the most various goals through algorithmic intermediation. Usually, the relationship between users and platforms is grounded in a deal. Users are in search of a connection to other users for the most diverse reasons: cultural, commercial, social, or political. Platforms, on the other hand, provide this intermediation in exchange for access to data that will give them some economic advantage. Just as infrastructures, platform businesses establish context to enable, support, and afford certain practices, at the same time that they hinder or prevent others, and upon which other online services rely.[75] Thus, Uber is a platform because it can connect individuals that own a car and want to receive financial compensation for driving

[70] SRNICEK, op. cit., p. 77.
[71] According to Forbes' list of the world's most valuable brands in 2019, the top 5 is dominated by the five biggest technology companies, Apple, Google, Microsoft, Amazon, and Facebook, from which three of them are service providers. THE WORLD'S Most Valuable Brands. **Forbes**, [s.l.] Apr. 4, 2020. Available at https://www.forbes.com/powerful-brands/list/. Last access Jun. 30, 2020.
[72] GILLESPIE, Tarleton. The politics of ' platforms '. **News Media & Society**, v. 12, n. 3, p. 347–363, 2010, p. 349-350.
[73] Id.
[74] LYNSKEY, Orla. Regulating ' Platform Power '. LSE Law, Society and Economy Working Papers No. 1/2017. Available at < https://ssrn.com/abstract=2921021>. Last access on Aug. 4, 2020.
[75] WOOD, David Murakami; MONAHAN, Torin. Editorial: Platform surveillance, **Surveillance, and Society**, v. 17, n. 1–2, p. 1–6, 2019, p. 3. VAN DIJCK, José; NIEBORG, David; POELL, Thomas. Reframing platform power. **Internet Policy Review**, v. 8, n. 2, p. 1–18, 2019.

others somewhere (drives) and individuals that are willing to pay to be taken to some specific place (passengers). Netflix, on the other hand, cannot be regarded as a platform, because there is no exchange or interaction between users. It is just a media service provider transmitted through streaming technology. Such dynamic has many implications that will be discussed in the next pages of this work. For instance, the characterization of platform markets as two or multi-sided markets[76], which may bring some challenges in the analysis of anticompetitive practices.

One can also depict platforms as firms whose primary business consists in the extraction and processing of data.[77] Platforms can collect, transmit, and process huge amounts of data. The wealth accrued by this new wave of capitalists, however, does not come from the quality or nature of the data itself, but from the patterns that can be extracted, predicted, and inferred from them, and then turned into profit. Many scholars consider Google the pioneer company to turn information into profit.[78] At the end of the twentieth century, the excitement about the potentialities of the Internet brought an array of venture capital to Californian companies, hoping that many of them would boost rapidly and become a leader in this emerging market. Google, a search engine company, was one of these firms. It collected and analyzed the behavioral data from its users to constantly improve their search results and user experience. Nevertheless, no market operation in this cycle would generate profit. With the dot com bubble in the late 1990s, the pressure exerted by venture capital over Google, its engineers felt the necessity to find a profitable business model. In fact, there was a vast amount of behavioral data not useful to the improvement of the company's services, but which constituted a unique source of user's personal information. This freely available raw material discovered to be a potentially valuable asset[79] started to be used to make more accurate predictions about an individual's tastes, thoughts, and feelings, and then became a source of targeted advertisements sent to them.

---

[76] EVANS, David S., **Multisided platforms, dynamic competition, and assessment of market power for Internet-based firms**, Coase-Sandor Institute for Law and Economics Working Paper No. 753, March 2016, p. 6 ("A multi-sided platform is called multi because it provides a way for two, or more, types of participants to get together. It is called a platform because it typically operates a physical or virtual place that enables these different types of agents to interact. Each side of the platform consists of the participants who have the option of using the platform to connect. […] Multi-sided platforms typically reduce frictions that get in the way of economic agents finding each other, interacting, and exchanging value on their own"). For an in-depth discussion about the challenges related to the regulation of two or multi-sided markets, see the discussion in Section 2.1, p. 44.

[77] SRNICEK, op. cit.

[78] Cf. LASTOWKA, Greg, Google's Law. **Brooklyn Law Review**, v. 73, n. 4, p. 1327–1410, 2008; MURRAY, op. cit.; ZUBOFF, op. cit.

[79] Shoshana Zuboff defines as "behavioral surplus" this the vast amount of data that was not primarily used to improve Google's services. ZUBOFF, op. cit., p. 55.

AdWords, Google's selling advertiser program, shortly became companies' main source of profit, as it revealed to be extremely attractive to sellers be able to nail people that would more likely be receptive to their products, leading to higher efficiency and more guaranteed outcomes.[80] For this process to be virtuous, though, platforms supervise users' activities and stimulate interactions on their websites, as the more they interact, the more data is recorded and collected. The outstanding and highly profitable business model initiated by Google was later replicated by various companies from different economic sectors with the construction of enormous databases through an unprecedented accumulation of data as raw material as well as the extensive development of data science and machine learning techniques for converting and processing voluminous flows of data.[81] Thus, although accumulation and ownership of data will characterize the capitalists of the digital age, property of means of production, here, code (hardware and software) will also play an important role in this new step of capitalism. The collection of data is an important aspect in the design of the best codes, because the more and diverse data one has, the better he or she will improve the code.

The creation of metadata by search engines such as Google, based on behavioral data extracted from users that would be later sold to advertisers is just one strand of the platform's business model. Platforms may also operate renting their digital infrastructure to third companies and gathering data for their uses.[82] The most notorious example is the cloud computing services offered by Amazon Web Services, although Google Cloud Platform - GCP, Microsoft's Azure has also been competing in this market.[83] Other platforms serve as a place of exchange between workers, suppliers, and customers, such as Uber, Airbnb, and TaskRabbit. Although they do not own any means of production, they own the algorithm and pay their partners by task. Traditional industrial companies are also developing new processes with platform characteristics. In this case, however, data is majorly collected and processed to make production more efficient through the use of sensors and computer chips to machine to machine communication and exchange of data without human interaction[84]. The challenge here is to

[80] Id. at 55-56.
[81] SOLOVE, Daniel J. **The Digital Person: Technology and Privacy in the Information Age**. 1 ed., New York: New York University Press, 2004 ("There are hundreds of companies that are constructing gigantic databases of psychological profiles, amassing data about an individual's race, gender, income, hobbies, and purchases. Shards of data from our daily existence are now being assembled and analyzed—to investigate backgrounds, check credit, market products, and make a wide variety of decisions affecting our lives").
[82] SRNICEK, op. cit., p. 98.
[83] VELLANTE, David. Breaking Analysis: How AWS, Azure, and GCP Compete for Cloud Leadership in the 2020s. **Wikibon**, Feb. 9 2020, Available at https://wikibon.com/breaking-analysis-how-aws-azure-and-gcp-compete-for-cloud-leadership-in-the-2020s/. Last access on July 2, 2020.
[84] SRNICEK, **Platform Capitalism**.

establish patterns for communications and interoperability between components, a job that has been performed by industrial internet platforms such as Cisco, Siemens. GE and IBM.[85] Similar to cloud platforms, they extract data to improve processes and to develop better services and products for their customers.

The next section will be devoted to analyzing through what strands and how platforms exert their power. According to Lessig, the most efficient way to regulate behavior online is through architecture (code), which means that ownership and knowledge to manipulate it is a fundamental part of control.[1] Thus, in order to understand how platforms exert control over the networks, it is necessary to analyze how they operate the code. This analysis is especially important for the next chapters of this work because it helps to identify in which realms regulatory authorities can act over those companies. Lina Khan considers that are three sources of platform tech power: gatekeeping power, leveraging, and information exploitation.[86] Differently from Khan, in the next section, I will focus on explaining how platforms exert their power through their gatekeeping position and their surveillance apparatus, as leveraging seems to be a consequence of the exercise of gatekeeping power. Then, I will explain how the two forms of power analyzed –surveillance and gatekeeping - intertwine.

1.3 THE MEANS THROUGH WHICH PLATFORMS EXERCISE THEIR POWER

Power, as explained by Manuel Castells, is the capacity of a social actor to influence another one asymmetrically, so that the empowered actor will have their interests, wills, and values favored.[87] The existence of power necessarily implies the existence of a relationship, as power is always exerted relationally, being this relationship asymmetric, with one actor subject to the interests, wills, and values of another.[88] Due to this asymmetry, power has long been understood in verticalized relationships[89] and traditionally related to sovereignty, the authority of a state to rule over those who are in a territory through the monopoly of violence. However, this model, in which a state exerts its authority through the enactment of laws, started to be eroded with the rise of the global networks. In this process, diagnosed by Joel Reidenberg as a

[85] SRNICEK, op. cit., p. 101-103.
[86] KHAN, Lina M., Sources of tech platform power, **Georgetown Law Technology Review**, v. 2, n. 2, p. 325–334, 2018.
[87] CASTELLS, op. cit., p. 10.
[88] Id.
[89] Michel Foucault explains that power also operates in a capillary level of social relationships, horizontally. Although one of the actors exerts its influence over the other, the one subjected is not unpowered and can always offer some degree of resistance. FOUCAULT, Michel. **Discipline and punish:** the birth of the prison, translated by Alan Sheridan. New York: Pantheon, 1977.

disintegration of the traditional sovereignty paradigms, a single actor action can transcend a country's borders and regulations from different states may overlap, while traditional categorizations of law are incapable to regulate properly behavior online.[90] However, it does not lead to a cyberlibertarian approach in which the Internet is perceived as a lawless place. New borders emerge through private agreements and network architecture, with users being subject to rules of membership and behavior that govern the online communities they belong.[91]

The emergence of the online network – and the problems that derive from this s leads to two formulations proposed by Lessig: in the digital age, private actors gain relevance as regulators rather than regulated, and the main mechanism of control is the code rather than the law or social norms.[92] Architectures of control, though, can be smoother in some circumstances than in others. In this context of prevalence of code, platforms become important regulators of the Internet. As platforms are inherently a place of exchange, they have a strong capacity to structure and maintain networked communities where users will spend a significant amount of their time online. Besides, the architecture of networks offers a high level of configurability, and functions as an effective mean to regulate behavior online, which means that code functions as law.[93]

As seen in the last section, despite the technical aspects involved in the construction of networks, the code reproduces political and economic power, reflecting the goals, priorities, and wills of its owner.[94] Through code, platforms have the capacity to regulate access and circulation of information, influence nodes' behavior, and impose the values of the network, exerting a gatekeeping power. The choice to work with the concept of gatekeeping rather than others such as 'platform power' or 'market power' is justified by the fact that it explains better the phenomenon in which actors exert dominance over a network. Cohen considers that in the context of informational capitalism the term 'market power' does not address the risks that emerge from the digital ecosystem.[95] Platforms operate in two or multi-sided markets, in which one of the sides of the market usually does not pay a price or pays a very small price for the service provided. However, users who have access to these platform services are subjected to

[90] REIDENBERG, Joel R, Governing Networks and Rule-Making in Cyberspace, **Emory Law Journal**, v. 45, p. 911–930, 1996. Lessig also expresses the regulatory difficulty related to competing sovereigns of "cyberspace laws" and "real-world laws", LESSIG, op. cit., p. 26-28.
[91] REIDENBERG, op. cit.
[92] LESSIG, op. cit.
[93] Id. For a detailed framework about regulation of speech by private online platforms under the First Amendment, cf. KLONICK, Kate. The New Governors: The People, Rules, and Processes Governing Online Speech. **Harvard Law Review**, v. 131, p. 1598–1670, 2018.
[94] COHEN, op. cit., p. 3.
[95] COHEN, op. cit., p. 174-175.

massive extraction of personal data, having little awareness about what can be done with their information and the risks involved in these operations. According to Cohen, this situation brings some difficulties to traditional antitrust law doctrine, which heavily relies on price analysis but does not easily monitor other aspects related to the quality of services, so she prefers to refer to 'platform power' rather than 'market power', although admitting that there is no consensus about the definition of 'platform power.[3] Despite Cohen's lucid diagnose, the concept of gatekeeping affords more clarity. First, because it focuses control over networks and information flows rather than on the technology (platform).[96] Secondly, gatekeeper theory relates to power over information flows as well as control over access in a network and the relationship between gatekeepers and nodes.[97] Thus, it can relate to not only economic harms (competition harms), but also social (censorship, workers' exploration) and political harms (election engineering). On the other hand, whereas individuals hardly have total control of the information they provide on the Internet, those who can collect, store, and process data influence information flows and, depending on their capacity, may function as gatekeepers. In this sense, qualitative and quantitative accumulation of data is essential for the improvement of code and control of networks. As appointed by Zuboff, it was only after the discovery of behavioral surplus that Google managed to build a lucrative business model. Thus, the capacity to efficiently control networks is intrinsically related to the information provided by the dominance of surveillance mechanisms.

1.3.1. GATEKEEPER

As seen in the first section of this chapter, in the network society some of the nodes have a predominance over others given their capacity to decide what information will travel through this environment and in what circumstances. They act as intermediaries, building bridges between those who produce information and those who consume it. This gatekeeping function, though, should be viewed from a relational perspective. Depending on the context, actors in a network may exercise different forces and have different influences concerning one another. In the broad Internet environment, many players can be identified as gatekeepers, from content moderators in portals to Internet service providers - ISPs. When comparing to content moderators, ISPs exercise a stronger gatekeeping function, as they are responsible for users' access to the Internet, but when looking at content moderation performed in an online portal, it

[96] Ibid., p. 9.
[97] Ibid., p. 10-11.

can filter, delete users comments as well as control who can and who cannot comment on a certain post. Similarly, although gatekeeper power may refer to a range of controls exerted on a network, from content filtering to participation in certain markets, as this work regards the role of the FTC as the regulatory authority in competition and consumer privacy, in this section I will focus primarily on the relationships between various actors in digital markets.

Online platforms such as Google and Facebook with billions of users worldwide are among the most accessed sites on the Internet, but differently from other high traffic portals, they are sites of exchange: opinions, consumption, services, visions, projects. With a significant amount of information flowing through them, allowing to perform a significant gatekeeping function, filtering and programming their users' experience, and shape discourse and public opinion. Whereas traditional companies buy raw material, produce their products, and sell them to consumers with a single demand, digital platforms sell access to participants of one group with a certain demand to participants of one or more different groups with their demands. As result, rather than merely nodes in the network, some platforms replace both the marketplace and the public square, even turning into the networks themselves. Therefore, it enables companies to exert their gatekeeping power over users in two ways. First, through a logic of inclusion/exclusion, in which they exercise gatekeeping power to bar access or those who do not aggregate value to the network or jeopardize their dominant interests.[98] Second, through their ability to program and reprogram the network in order to pursue their own goals, and to connect (or not) different networks.[99]

The exercise of such powers inherently relates to their number of users and of connections, a phenomenon called "network effect", in which the number of users of a product or a service is related to the value of this service or product. Network effects can be direct or indirect. Direct network effects occur when the value of the product or service increases as new users join the network. Just as it has become more significant to have a telephone as the number of telephone line holders expanded, a social network will be more valuable and influential if it aggregates a significant number of users. Indirect network effects (or cross-group effects) happens when the value of the network depends on users from different groups joining the network. In platforms such as Uber and Airbnb, there must be drivers and house owners willing to offer their services as well as passenger and guests demanding the service. Indirect network

[98] Castells calls this form of power "networking-making power". CASTELLS, op. cit., 2009, p. 45.
[99] Castells calls this form of power "networking-power", CASTELLS, op. cit., 2009, p. 42. According to Julie Cohen, platforms function both as networks and as infrastructure, as they control the flow of information over nodes (users) and are the grounds for the development of other goods. COHEN, op. cit., 2019, p. 47-48. Nick Srnicek also sees platforms as digital infrastructures that allow groups to interact. SRNICEK, op. cit., .p. 78.

effects are very characteristic of multi-sided markets and are extremely relevant to the understanding of platform dynamics. In this sense, depending on the size of the network, an individual may not have significant benefits from joining it. On the other hand, be or remain excluded from the same network can be extremely harmful. Network owners in such circumstances may have far-reaching gatekeeper power.

The question of access to the services and compliance to the rules provided by platforms is one of the most sensitive regarding the economic power of these companies, especially when it regards platforms that are in a very privileged position on the market. The dispute between Epic Games, owner of the worldwide popular game Fortnite, and Apple illustrates well this issue: iPhone users must use Apple's App Store to download apps and to make payments related to games purchased in the store, which grants Apple a 30% fee in every transaction. Circumventing App Store's payment network, Fortnite implemented its in-app payment system[100]. In retaliation, Apple banished Fortnite out of its store for violation of App Store guidelines, which led Epic Games to file a lawsuit against Apple's exclusion as well as against Google due to Google Play Store's similar policies.[101] Epic argued that Apple maintains a monopoly on iOS enables devices and practiced exclusionary conduct by prohibiting the use of alternative methods of payment. Both Apple and Google hold a very powerful position in mobile software distribution.[102] Currently, app developers can only access the market through two stores: iPhone users if you are in the App Store; Android users, if you are in the Google Play Store, being extremely difficult for developers, especially small developers, to stand against any policy enacted by these two companies. On the other hand, simply leave these two stores would be extremely burdensome for many of the developers, considering that the cost to produce and distribute tangible copies of the games throughout the country, or the world, is substantially higher. Indeed, such kind of action undertaken by Epic was only possible because Fortnite was an astonishing financial success that brought $1.8 billion in revenues to Epic just in 2019,[103] allowing Epic to fight with similar weapons a lawsuit against Apple. Nevertheless,

[100] GARTENBERG, Chaim. Epic's Fortnite standoff is putting Apple's cash cow at risk. **The Verge**, [s.l.], August 17 2020. Available at https://www.theverge.com/2020/8/17/21369460/apple-fortnite-app-store-services-business-model-epic-games. Last access Aug. 25, 2020.

[101] STATT, Nick. Apple just kicked Fortnite off the App Store. **The Verge**, [s.l.], Aug. 13 2020. Available at https://www.theverge.com/2020/8/13/21366438/apple-fortnite-ios-app-store-violations-epic-payments. Last access on Aug. 25, 2020.

[102] In 2020, Android users corresponded to 84.1% of the operating system market share, while iOS to 15.9% market share. SMARTPHONE market share. **IDC,** [s.l.], Apr. 28 2021. Available at https://www.idc.com/promo/smartphone-market-share/os. Last access Jun 4, 2021.

[103] GILBERT, Ben. 'Fortnite' made $1.8 billion in 2019, analysts say – that's down 28% from 2018, but it's still the biggest game in the world. **Business Insider**, [s.l.], January 3 2020. Available at <https://www.businessinsider.com/how-much-did-fortnite-make-in-2019-2020-1>. Last access on Aug. 25, 2020.

this example demonstrates how hard can be for the majority of developers not to comply or disagree with platforms policies, as they do not have deep pockets like Epic, and these platforms are today an important bridge to reach consumers. The lawsuit is still pending in the United States District Court for the Northern District of California.

The value – and power - of a platform network also lies in its capacity to attract and retain users, functioning as 'attention seekers'[104] in a time marked by information overload. In order to keep themselves relevant, platforms must remain as an indispensable point of intermediation and attention for parties,[105] creating an environment in which they offer a wide variety of desirable and useful services, some of them free or below their cost.[106] When a user creates an account in any of these online services, he or she has almost automatically access to a range of additional ones provided by these companies. With a Google account, an individual has access not only to Gmail but also to a range of services, such as Google Drive, Google Docs, Google Hangouts YouTube, Google Maps, and others. Similarly, an Amazon account grants access to applications such as Kindle, Twitch, and Audible. However, the easy access to various services stimulates users to keep up with them, as they are usually integrated and/or are included in the same pack of services offered at a generous price. As consequence incentives to users give a try to new services can turn more costly. The tendency, though, is that companies control at least one product or service that will guarantee continued high profits to be invested both in their core business and in promising new markets.[107] In recent years, vertical acquisitions and mergers allowed many platforms to substantially grow and become genuinely technology conglomerates through the acquisition of startups. Silicon Valley companies like Google and Facebook, although have been major sponsors of many emerging tech startups in recent years,[108] also have been accused of market distortions due to their systematic policy of buying emerging companies in strategic realms, such as artificial intelligence and machine learning, leaving little room for competing entrants, so they do not menace their dominant position.[109]

---

[104] EVANS, op. cit.

[105] Consider Google's mission statement: "organize the world's information and make it universally accessible and useful". Think about how internet access nowadays is shaped by search results by Google. GOOGLE. **About Google**. Available at <https://about.google/>. Last access on Sep. 28 2020.

[106] BARWISE, Patrick; WATKINS, Leo. The evolution of digital dominance: how and why we got to GAFA. *In*: MOORE, Martin; TAMBINI, Damian (Orgs.), **Digital Dominance: the power of Google, Amazon, Facebook, and Apple**, New York: Oxford University Press, 2018, p. 25-26.

[107] BARWISE, Patrick; WATKINS, Leo., op. cit., p. 22-24.

[108] SRNICEK, op. cit., pp. 93-94.

[109] BRANDOM, Russel. The monopoly-busting case against Google, Amazon, Uber, and Facebook. **The Verge**, [s.l.], Sep. 5, 2018. Available at <https://www.theverge.com/2018/9/5/17805162/monopoly-antitrust-regulation-google-amazon-uber-facebook>.

The question of interoperability is another critical aspect of gatekeeping power exerted by platforms that imply high switching costs. Generally, interoperability refers to "the ability to transfer and render useful data and other information across systems (which may include organizations), applications, or components". [110] Horizontal interoperability refers to the capacity of two or more different systems to communicate with one another, such as interconnection between communications networks, while vertical interoperability corresponds to the ability of certain products, services, and networks to connect with complementary ones.[111] It refers to the capacity to share content through different networks, such as Kindle e-books that can only be read in the Kindle app and Kindle format, or songs bought in iTunes that are only played on Apple devices. In competitive markets, consumers may choose more or less interoperable systems or devices depending on the characteristics they are pursuing. Devices or systems with a higher interoperability degree tend to have reduced costs and lower costs whereas those with a lower degree of interoperability may offer higher innovative products that require specific components or better quality complementary products through the control of the value network.[112]

Problems, however, may appear in markets with winner-takes-all tendencies, such as platforms markets, due to the risk of dominant firms decide unilaterally on the interoperability of products, as occurred in the Microsoft case under the European Union law. [113] Sun Microsystems, Microsoft's competitor in the workgroup server market, filed a complaint accusing Microsoft of abusing its monopoly power on the PC operating system market, by refusing to supply relevant interface information about its PC operating systems. Basing on 'essential facilities' doctrine[114] and relying on article 82 of the Treaty establishing the European Community,[115] which defines as unlawful the abuse of dominant position, the EU Commission

[110] GASSER, Urs; PALFREY, John G. **Breaking down digital barriers: when and how ICT interoperability drives innovation**. Berkman Center Publication Series, 2007, p. 4. Available at <https://dash.harvard.edu/bitstream/handle/1/2710237/Breaking%20Down%20Digital%20Barriers.pdf?sequence=2&isAllowed=y>. Last access Aug. 17, 2020.

[111] KERBER, Wolfogang; SCHWEITZER, Heike. **Interoperability in the digital economy**. **JIPITEC** v. 8, 2017, 39-58, p 56-58.

[112] KERBER; SCHWEITZER, op. cit., p. 7.

[113] EUROPEAN UNION. European Court of First Instance. Microsoft Corp. v. Commission, T-201/04, Sep. 17 2007. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62004TJ0201.

[114] The essential facility doctrine was developed in the United States and adopted with a degree of modification in foreign legal systems such as the European Union and the United Kingdom. Under this doctrine, a monopolist who owns access to a facility must provide reasonable use of such facility. UNITED STATES. Supreme Court. United States v. Terminal Railroad Association, 224 U.S. 383 (1912). Apr. 22, 1912. Available at < https://supreme.justia.com/cases/federal/us/224/383/>. Last access on Aug. 30, 2020.

[115] Treaty Establishing the European Community art. 82, Nov. 10, 1997, 1997 O.J. (C340) 3.

held that Microsoft conduct was abusive, as it curbed competition due to the essentiality of the information for the development of products, limiting development and harming consumers. The EU Commission obliged Microsoft to disclose Windows interfaces for competing networking software firms and fined Microsoft 497 million euros.[116]

Uprising technology startups face similar interoperability questions with regard to data access. Big technology companies offer a variety of services that enables the collection of a greater and more diverse amount of user data. Besides, as seen previously, established platforms usually have the financial means to undertake acquisitions of emerging companies. This practice allows these platforms to offer a new kind of service and, consequently, a new mean to collect or process information. Large-scale data collection is essential to continuous service improvement and personalization, which drives big platforms to extend their apparatus into new realms even apart from their core business.[117] The better companies can understand how their users think and act, the better they provide services tailored to their users' needs and offer solutions in realms such as advertising. All this taken together creates a cycle in which users tend to remain using these services, as switching costs will be high, leading those firms to consolidate dominant positions in the market. As consequence, there is an enormous concentration of data in the hands of very few companies. As data is the most valuable asset in information capitalism, platforms claim ownership over personal data denying sharing with smaller companies that would benefit from it and create new products and services.

However, if, on the one hand, the management of personal data by a small number of technology firms raises concerns regarding freedom in its most broad meaning and self-determination, on the other interoperability may raise privacy concerns as it increases the number of parties that would have access to personal information. Nonetheless, interoperability enthusiasts argue that it is not interoperability *per se* that increases privacy risks, as it can "deprive companies of their discretion over when they share data and with whom".[118] They

---

Any abuse by one or more undertakings of a dominant position within the common market or in a substantial part of it shall be prohibited as incompatible with the common market in so far as it may affect trade between the Member States. Such abuse may, in particular, consist in:
(a) directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions;
(b) limiting production, markets, or technical development to the prejudice of consumers;
(c) applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;
(d) making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts.

[116] EUROPEAN UNION. European Court of First Instance. Microsoft Corp. v. Commission.

[117] SRNICEK, Nick, The challenges of platform capitalism, **Juncture**, v. 23, n. 4, p. 254–257, 2017.

[118] CYPHERS, Bennet; DOCTOROW, Cory. Privacy without monopoly: data protection and interoperability. Electronic Frontier Foundation, [s.l.] Feb. 12 2021. Available at: https://www.eff.org/wp/interoperability-and-privacy#Risksandmitigations. Last access Mar. 1, 2021.

argue that data interoperability may represent the opportunity for users to take back control over their data, with them having true knowledge of data stored and autonomy to transfer it elsewhere. These regulatory measures, thus, would have the potential to foster competition and stifle a more democratic online environment. Interoperability, though, depends on the design to its implementation, either through organizational or legal tools, such as the European privacy regulation.[119] Article 20 of the General Data Protection Regulation 2016/679[120] ensures the right to data portability, which may help to overcome the lock-in effect and increase user mobility.[121]

In a market where users' attention is a disputed asset, these companies distinguished from others similar due to their capacity to not only the collection of information but also to analyze an immense contingent of information have become one of most profitable activities. However, the information gathering that characterizes platform business models requires a sophisticated apparatus for data extraction. Therefore, the development of surveillance techniques reveals as an indispensable gear in the expansion of gatekeeper power. This subject is to be explored in the next section.

1.3.2 SURVEILLANCE

From workplaces to homes, streets, shopping carts, banking transactions, communications, internet, bodies: surveillance is ubiquitous. Although there is no definitive concept of surveillance, scholarship widely adopted David Lyon's definition of surveillance as "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction".[122] Thus, surveillance practices have been conceived as

[119] GASSER; PALFREY, op. cit., p. 16.

[120]Article 20 GDPR: "The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); (b) the processing is carried out by automated means. 2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible. 3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. 4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others".

[121] KERBER, WOLFGANG; SCHWEITZER, op. cit., p. 20.

[122] LYON, David. **Surveillance studies: an overview.** Cambridge: Polity, 2007, p. 14 ("Surveillance directs its attention in the end to individuals (even though aggregate data, such as available in the public domain, may be used to build up a background picture). It is focused. By systematic, I mean that this attention to personal details is not random, occasional, or spontaneous; it is deliberate and depends on certain protocols and techniques. Beyond this, surveillance is routine; it occurs as a 'normal' part of everyday life in all societies that depends on bureaucratic

more than just watching; they are connected to the ability to modulate and control behavior.[123] With information becoming central to the functioning of corporations and governments and for them to make decisions, surveillance practices define how modern institutions operate.[124] In a regime of informational capitalism, in which the economy is orientated towards the collection, processing, and analysis of information, surveillance practices emerge as an important foundation of this new stage. The persistent and ubiquitous monitoring of persons and processes is critical to the identification of potential risks, opportunities, and trends, guaranteeing a greater profit predictability and gains of efficiency. The dominance of techniques to extract information places companies and public agencies with such expertise in a position of privilege, as other economic and social actors depend on the information provided by them to make decisions and build strategies. As consequence, surveillance implies a relationship of power in which watchers are few and privileged, while the watched are, most importantly, visible, subject to identification.[125]

In recent years, the intrusiveness of public and private actors in the everyday life has become a trendy subject and risen a concern over the privacy of individuals, especially after Snowden's revelations of United States espionage and Cambridge Analytica scandals regarding data manipulation, and even a debate of what privacy means nowadays. This is not a new phenomenon, though. Surveillance practices and methods have long existed but have a more sophisticated shape in modern societies. Social and economic processes such as industrialization, urbanization, and organization of workforce rose the necessity in the government to intensify surveillance not only to maintain control of the emerging urban mass but also to provide welfare policies to their citizens, as information gathering was necessary to know who would benefit from them and where they are.[126] The bureaucracy saw the necessity

---

administration and some kinds of information technology. Everyday surveillance is endemic to modern societies. It is one of those major social processes that actually constitute modernity as such.").

[123] James B. Rule, whose work has preceded Foucault's studies over discipline and control reconceptualizing Bentham's Panopticon, relates surveillance to "*the means of knowing when rules are being obeyed, when they are broken, and, most importantly, who is responsible (...) a second element of surveillance, also indispensable, is the ability to locate and identify those responsible for misdeeds of some kind*", RULE, James B., **Private lives and public surveillance: social control in the computer age**, London: Allen Lane, 1973, p. 21. Roger Clarke conceptualize surveillance as "*the systematic investigation and monitoring of the actions or communications of one or more persons*", CLARKE, Roger A, Information technology and dataveillance, **Communications of the ACM**, v. 37, n. 5, p. 498–512, 1988, p.499.

[124] MONAHAN, Torin; WOOD, David Murakami. Introduction: surveillance studies as a transdisciplinary endeavor. *In*: MONAHAN, Torin; WOOD, David Murakami (Orgs.), **Surveillance Studies - A Reader**, New York: Oxford University Press, 2018.

[125] LYON, op. cit.

[126] WELLER, Toni. The information state: a historical perspective on surveillance. In: BALL, KIRSTIE; HAGGERTY, KEVIN; LYON, David (Org.), **Routledge Handbook of Surveillance Studies**, New York: Routledge, 2012, p. 58.

not only to create an apparatus to minimally investigate and sort citizens as part of the procedures to provide public services but also to create personal information for them, such as individual passports and healthcare numbers.[127] On the other hand, the United States and European governments created in the late nineteenth-century secret service agencies as governmental apparatus to gather and monitor information related to individuals that would constitute a menace to national security.

Since then, those agencies suffered a huge expansion in their purviews, especially during the World Wars and later throughout the Cold War, historical periods characterized by massive defense spending.[128] More recently, the combat to terrorism and religious extremism has become justification for the expansion of government techniques and practices related to the extraction, collation, and analysis of data to the identification of potential threats and control of populations. Recent developments in information technology and the decrease of costs enabled governments to employ unprecedented surveillance techniques to monitor citizens based on the gathering of personal information. It is important to note, though, that surveillance is not homogeneous, and its level may vary in intensity depending on the group watched. Terrorists and dangerous criminals are drowned more attention than ordinary citizens. In this sense, automatization enabled the development of new procedures for the selection and sorting of individuals, giving birth to a new form of governance called the National Surveillance State. The National Surveillance State emerges as a successor of the Welfare State, characterized by the recognition of social and economic rights to people, and the National Security State, whose underpinnings lie in the massive expenditure in national defense and military, in which the government collects an enormous amount of data to identify potential threats and deliver social services.[129]

Notwithstanding, if the dangers and fears to autonomy involving surveillance are traditionally related in popular culture to state authoritarianism, in the rise of the information society, private actors – platforms, data brokers - emerge as responsible for a significant part, if not most, of surveillance practices. Public agencies and private companies then developed a symbiotic relationship, in which both parties mutually benefit. Platforms that flourished with

---

[127] WEBSTER, William R.. Public administration as surveillance. In: BALL, Kirstie; HAGGERTY, Kevin D; LYON, David (Orgs.), **Routledge Handbook of Surveillance Studies**, New York: Routledge, 2012, p. 314.
[128] WELLER, op. cit., p. 61.
[129] BALKIN, Jack M. The Constitution in the National Surveillance State. **Minnesota Law Review**, v. 93, n. 1, p. 1–25, 2009 ("The National Surveillance State is a permanent feature of governance, and will become as ubiquitous in time as the familiar devices of the regulatory and welfare states. Governments will use surveillance, data collection, and data mining technologies not only to keep Americans safe from terrorist attacks but also to prevent ordinary crime and deliver social services. In fact, even today, providing basic social services-like welfare benefits-and protecting key rights-like rights against employment discrimination-are difficult, if not impossible, without extensive data collection and analysis").

the advent of information capitalism manage great amounts of data as raw material, so they are constantly updating and refining their procedures to extract as much users' information as possible in order to amplify their analysis and increase their prediction capacity of users behavior. Although retaining the monopoly of the use of force, governments associated with those firms to, on one hand, outsourcing to them the task of extraction and analysis of data, and, on the other, financing private innovation in surveillance methods and developing direct technology for this purpose.[130] The great vantage of this private enforcement system relies on the absence of constitutional restrictions usually imposed on state actors related to speech and privacy of communications.[131]

Such association between public and private actors is not only restricted to national security matters, though. The government, through either the enactment of statutes or its agencies' action, has delegated the role of monitoring certain groups or certain kinds of infringements, such as copyright infringements. In the context of 'privatized panopticons', the State does not regulate directly through the law but seeks out private actors with control of information flows on the Internet to prevent infringement through private surveillance mechanisms.[132] In this sense, Boyle already criticized in the 1990s the jurisprudence of digital libertarianism for opposing sharply to public direct regulation of the Internet, but not realizing that there are other indirect and effective means of monitoring behavior online through private actors.[133] Similarly, Lessig was also concerned with the architecture of cyberspace that both government and commercial internet were building. He argued that such architecture, the code, should be embedded in constitutional values and reflect individuals' liberties conquered through centuries of struggle.[134] Without any kind of regulation, cyberspace, in his view, would not keep its promise of freedom - "left to itself, cyberspace will become a perfect tool of control".[135] Years later, Zuboff pointed the cyberlibertarian resistance to public regulation of the Internet as one of the factors that favored the emergence of surveillance capitalism.[136]

---

[130] HAYES, Ben, The surveillance industrial complex, *In*: BALL, KIRSTIE; HAGGERTY, KEVIN; LYON, David (Org.), **Routledge Handbook of Surveillance Studies**, New York: Routledge, 2012. For a brief explanation of the cooperation undertaken by Google and United States' Intelligence Community Agencies post-9/11 events, *see* ZUBOFF, op. cit., p. 80-82.
[131] BALKIN, op. cit.; PASQUALE, op. cit.
[132] BOYLE, James, Foucault in cyberspace: surveillance, sovereignty, and hardwire censor, **University of Cincinnati Law Review**, v. 66, p. 177–205, 1997, p. 195-201.
[133] Id.
[134] LESSIG, op. cit., p. 6.
[135] Id.
[136] ZUBOFF, op. cit.

Private sector surveillance does not function exclusively as a long hand of government, though. Rather, as seen in the previous sections, data extraction undertaken by platforms is a central engine of informational capitalism, and the comprehensiveness and variety of information gathered by them have only been possible given the continuous, systematic use of surveillance practices over users. Despite some differences in the structuring of platforms' business models, all of them follow an "extraction imperative" or "data imperative" to the point that data extraction should be as comprehensive as possible, from as many sources and as varied as possible.[137] Cohen considers that practices to extract and process personal data constitute a new type of public domain, which she names "biopolitical public domain", a set of abundant raw material (data) publicly available about which there are no prior claims[138]. It is biopolitical because it involves activities related to data processing and management with the intent to map and monetize populations.[139] The biopolitical public domain consists thus a realm that no one can object ownership to legally, although potentially valuable. Harvesting this raw material from the biopolitical public domain, platforms build detailed profiles containing information about her purchases, website activity, health, political orientation, interest, and lifestyle in the form of digital dossiers.[140]

If at the beginning of the Internet monitoring techniques such as cookies laid the groundwork for online commercial surveillance, with companies tracking users browsing activity[141], it turned necessary to develop more sophisticated processes and methods of data extraction, with the collection of information from the offline world, through the popularization of smartphones, personal assistants, and facial recognition systems. With such technologies, platforms are capable to transform into data the features that characterize each individual as a unique human being, such as voice, fingerprints, emotions, and way of walking. Individuals, thus, remain permanently connected and transmitting continuously information about their daily activities. Besides, surveillance may be justified as a key ingredient to deliver

[137] Id. FOURCADE, Marion; HEALY, Kieran, Seeing like a market, **Socio-Economic Review**, v. 15, n. 1, p. 9–29, 2017.
[138] COHEN, op. cit., 2019, p. 56.
[139] Id.
[140] SOLOVE, op. cit., p. 5.
[141] Cookies were first used in the Netscape browser as a small piece of data to identify visitors to a website. They are useful for remembering information about a website, such as login, items in the shopping cart, preferred language. Some of them can stay active and track user's behavior online for, later, offering targeted advertising. For a brief explanation about how cookies function, *see* ANON, Dennin, How cookies track you around the web and how to stop them. **Priavacy.net,** [s.l.] Feb. 24,2018. Available at <https://privacy.net/stop-cookies-tracking/>.

personalization and customization of goods and services, being Amazon's Alexa the pivotal example of such strategy.[142]

Nevertheless, it is not only a matter of extraction but also about prediction capacity. As extraction of data becomes insufficient for high-quality predictions, being necessary to improve the processing capacity to achieve better results in markets for future behavior.[143] In the platform economy, data function as an input for artificial intelligence and machine-learning methods that will, through highly sophisticated algorithms, reveal patterns of users' behavior. Patterns that later either will be directly sold to third parties or will serve as inputs of their services and products. They operate transforming raw data into refined data doubles[144] to generate expected behaviors.[145] However, differently from Orwell's 1984 novel and of Bentham's panopticon would suggest, platforms do not have interest in consumers feeling watched, so they gather personal information as discreet as possible, functioning as a one-way mirror, independently from users' awareness or explicit consent.[146] Both the construction of this 'sensing net' – a set of networked digital artifacts - and the sublimation of consent in coded environments work to generate a vast amount of data available in the public domain as a zone of free appropriation.[147] To accomplish this task of extraction information businesses make a series of design choices, from establishing default settings and making the path to change them non-intuitive to the configuration of templates that influence the way users to deal with content delivered to them.

On the other hand, the ability to predict patterns of consumer behavior creates a competitive advantage in the capitalist system, insofar as more accurately a company can predict, infer information about people through the data collected, the more it will be able to offer the products they need, the time they need, gain their confidence, and profit from that.[148]

---

[142] WEST, Emily, Amazon: surveillance as a service, **Surveillance & Society**, v. 17, n. 1/2, p. 27–33, 2019, p. 29.
[143]Zuboff introduces the "prediction imperative" as the second economic imperative of surveillance capitalism. ZUBOFF, **The Age of Surveillance Capitalism: the fight for a human future at the new frontier of power,** p. 132-133.
[144] HAGGERTY, Kevin D; ERICSON, Richard V, The surveillant assemblage, **The British Journal of Sociology**, v. 4, n. 51, p. 605–622, 2000.
[145] COHEN, op. cit., 2019, p. 84. Zuboff enumerates three approaches of economies of action to modifying users' behavior: "tuning", "herding" and "conditioning". Cf. ZUBOFF, op. cit., p. 187-190.
[146] ZUBOFF, op. cit., p. 58. PASQUALE, op. cit., 2016, p. 9.
[147] COHEN, op. cit., 2019, p. 57-58.
[148] STUCKE, Maurice E; GRUNES, Allen P, **No mistake about it: the important role of antitrust in the era of big data**, University of Tennessee Legal Studies Research Paper No. 269, 2015. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2600051. ("Companies undertake data-driven strategies to obtain and sustain competitive advantages. Companies increasingly strive to gain a "big data advantage" over their rivals. One MIT-led study showed that the more companies characterized themselves as data-driven, the better they performed on objective measures of financial and operational results. "[C]ompanies in the top third of their

Indeed, the goal of sophisticated predictive analyses is not simply to identify trends but find ways to modify them for the corporation's benefit. After all, it is the essence of capitalism to move towards gains of efficiency, with cut of costs and maximization of profit. In the field of advertisement, for instance, have been heavily relying on data to know better their target audience – through customer polls and market reports, for example – and, with information available, using techniques to grab consumers' fidelity.[149] The emerging problem is that the market of private surveillance is becoming increasingly concentrated in the hands of few platforms with global reach, which means that a selected group of firms is taking control of a great percentage of the world's data flows. Global corporations are naturally powerful actors, as they usually have privileged access to resources. In a mode of production in which data is the most important raw material, domination of Big Data analysis gives those companies an impressive power to either subside markets with metadata, like Google and Facebook, or providing machine-learning processes and infrastructure, as Amazon Web Services and Microsoft Azure. This creates a scenario in which different strains of businesses become dependent on these services to be competitive, such as appearing in the first pages of Google's or Amazon's search results. However, if competing with other services, platforms are placed in a very privileged position, giving their capacity to exert control over the networks through leveraging.

The use of mobile devices, big data, and the expansion of Internet of Things, are leading information societies towards ubiquitous computing, with the amplification of digital networks to every place, while the access to these networks tends to be more fluid, through the embedment of sensors to monitor everyday actions and the growing automatization of data processing and analysis. Commenting on the future of the web, Eric Schmidt, ex-CEO of Google and ex-chairman of Alphabet Inc., stated that "the Internet will disappear", as in the future there will be so many devices, sensors interacting with people that one will not even

industry in the use of data-driven decision making were, on average, 5% more productive and 6% more profitable than their competitors").

[149] Recall the bizarre case in which retailer Target inferred that one of its customers was pregnant, something that her father has not had notice yet. HILL, Kashmir. How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did, **Forbes**, [s.l.] Feb. 16 2012. Available at https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#4f9f5efb6668. Last access on Oct. 2, 2020. *See* also commenting on the Target case DUHIGG, Charles. How Companies Learn Your Secrets **The New York Times Magazine**, Feb. 16, 2012. Available at https://nyti.ms/AyNgCY. Last access on Oct 2, 2020. ("There are, however, some brief periods in a person's life when old routines fall apart and buying habits are suddenly in flux. One of those moments – *the* moment, indeed – is right around the birth of a child, when parents are exhausted and overwhelmed and their shopping patterns and brand loyalties are up for grabs. But as Target's marketers explained to Pole, timing is everything … the key is to reach them earlier before any other retailers know a baby is on the way").

realize it.[150] Such comprehensiveness of the information extracted brings to question whether those societies are moving from what James B. Rule names 'real surveillance systems*'* towards a scenario closer to a 'total surveillance society'.[151] In a total surveillance society, government amasses information about what all individuals are communicating and has mechanisms to foster social control. Rule claims that it is virtually impossible to implement such a level of awareness. In practice, real surveillance systems develop monitoring tools that come close to total systems, but they exert control over a limited number of people – e.g. terrorists – because the resources to supervise, such as personnel and computer processing capacity are finite.[152] However, with the development of services and devices, the increased interface between the online and real-world, and as algorithmically driven processes of data analysis are increasingly proficient in identifying "who is doing what and where", there is a growing concern about the possible harms it may cause both individually and collectively.

This unprecedented capacity of monitoring and extracting patterns of behavior undertaken by platforms has been a source of concerns related to privacy, consumer power, and self-autonomy and social inequalities.[153] In any period of economic history, the development of new technologies inherently brings new risks to society. Industrialization brought more quality of life with reduction of poverty and greater access to goods, but it has also resulted in an increase of pollution and diseases. In informational capitalism, the question of potential harms is particularly challenging as they are not always clearly visible or direct, as the vast majority of people remain largely in oblivion about how platforms to process and manipulate information, or use this knowledge to subside important decisions that will affect their lives, such as approval of health insurance or credit approval, or direct behaviors.[154] Moreover, technologies exert a great influence on social and cultural patterns, configuring how individuals understand the reality around them, even though processes related to access to information, social interaction remains quite opaque.[155]

---

[150] SMITH, Dave. Google chairman: 'the Internet will disappear'. **Business Insider** Jan. 25 2015. Available at https://www.businessinsider.com/google-chief-eric-schmidt-the-internet-will-disappear-2015-1. Last access on Oct. 2, 2020.
[151] RULE, op. cit.
[152] Id.
[153] ZUBOFF, op. cit. COHEN, op. cit**.** ANDREJEVIC, Mark, Automating Surveillance, **Surveillance & Society**, v. 17, p. 7–13, 2019.
[154] PASQUALE, op. cit., 2017.
[155] COHEN, Julie E. Configuring the networked citizen. *In:* SARAT, Austin; DOUGLAS, Lawrence; MERRILL UMPHREY, Martha (Orgs.), **Imagining New Legalities: Privacy and Its Possibilities in the 21st Century**, Stanford: Stanford University Press, 2012, p. 129–53.

When questioned about concerns related to data protection in the online environment, most people would like to have better control over their information circulating on the internet, although they do not behave accordingly (not using services that collect a massive amount of data, such as social networks, reading terms of use and privacy notices).[156] However, the challenge remains in the fact that individuals integrated into the digital economy are growing dependent on services offered by platforms, as some services provided by those companies make everyday life more comfortable, making it quite difficult to abandon their use.[157] If harms may occur due to the usage of those services, standing outside of them may bring other types of losses, such as social interaction and access to content. People feel powerlessness before the surveillance apparatus for collecting data and monitoring behavior, as they must choose between accepting confusing and obscure terms of use or give up using services that nowadays have increasing importance in our lives, which is seen as a symptom of the 'big data divide' between sorters and "sortees".[158] Zuboff also explores this powerless feeling when she explains the idea of a 'dispossession cycle', whose four stages encompass incursion, habituation, adaptation, and redirection.[159] This cycle begins with surveillance capitalists' unilateral incursion into private space – your laptop, your mobile phone, your photos, your interests, your face, your voice, your feelings – to extract behavioral surplus.[160] The second stage is habituation, which occurs when people conform with the incursion because it seems inevitable, while lawsuits and administrative enforcement stretch over time.[161] In a third stage, intermediaries are eventually obliged by public authorities to modify their practices but, through adaptation actions, these capitalists manage to comply superficially with governmental demands.[162] In the final stage of the dispossession cycle, there is a redirection of surveillance

[156] Around 79% of Americans are concerned about the way companies use the data collected, whereas 62% of Americans consider that it is not possible to go through daily life without having their data collected. AUXILIER, Brooke *et al.* Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. Pew Research Center, [s.l.] Nov. 15 2019. Available at https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/. Last access on Oc. 2, 2020.
[157] *See* FEDERAL TRADE COMMISSION. **Joint statement of FTC commissioners Chopra, Slaughter, and Wilson regarding social media and video streaming service providers' privacy practices**. File No. P205402 Dec. 14, 2020. Available at https://www.ftc.gov/public-statements/2020/12/joint-statement-ftc-commissioners-chopra-slaughter-wilson-regarding-social .
[158] ANDREJEVIC, Mark, The big data divide, **International Journal of Communication**, v. 8, n. 1, p. 1673–1689, 2014.
[159] ZUBOFF, op. cit.
[160] ZUBOFF, op. cit., at p. 96.
[161] Id.
[162] Id.

capitalists' operations, with reorientation for new rhetoric, methods, while they keep pursuing their goals.[163]

Surveillance relationships are also inherently asymmetric, as one part detains more information than the other and, because of that, rests in a position of advantage. Oscar Gandy depicts the imbalance between those responsible to make decisions based on data and those who will suffer the consequences of these decisions in the "panoptic sort", a mechanism to identify and classify individuals into categories and classes to control their access to goods and services.[164] Consumer profiling and sorting procedures orientate which opportunities, products, and services will be available, or not, to individuals based on their browsing history, the data collected from apps and devices. A job opportunity may be lost due to clicks on inappropriate web pages or undue "likes" on Facebook, one may be subjected to higher interests rates based on non-obvious aspects, such as his or her address, or even have your credit card rejected because you chose to fuel your car in a poor Californian neighborhood you are not used to transit.[165] Here behavior modification may occur not because of some nudge or inducement performed by an algorithm, but to not increase – or prevent decrease – of one's Übercapital, an index symbolic superiority based on digital traces collected from social media, credit bureaus, shopping history, and others.[166]

However, if social sorting is a powerful mechanism to evaluate risks, it may also replicate social and economic inequalities and institutionalize bias. Assessment of classifications tends to exclude the poorest members of society and minorities and may rise an invisible barrier to access some products and services. Moreover, sorting can emerge as a metric of moral judgment about individuals' personal choices: "spend, but in a controlled way. Drive, but not too fast. Eat, but stay healthy".[167] Indeed, classification systems are not new. Credit scores and insurance analysis are ordinary. Lack of transparency in collection and analysis criteria, usually justified by trade secrets, may lead to decisions absent of a visible or reasonable justification. Thus, only those who own the digital structure in which those processes are sustained or have the technical knowledge to operate it, have access to the outcomes generated

[163] Id.
[164] GANDY JR., Oscar H., **The panoptic sort: a political economy of personal information**, Boulder: Westview, 1993.
[165] Cf., e.g, ANDREJEVIC, op. cit., 2014, p. 1681; FOURCADE; HEALY, op. cit., p. 20-21. For an overview of the risks associated with big data analysis, cf. FEDERAL TRADE COMMISSION (FTC), **Big Data:** a tool for inclusion or exclusion? Understanding the issues. [Washington]: [s.n.], Jan. 2016. Available at https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report. Last access on Set. 2020.
[166] FOURCADE; HEALY, op. cit.
[167] FOURCADE; HEALY, op. cit.

by big data mining. This creates a division of learning in society, in which very few have expertise related to sorting processes.[168]

1.4 CONCLUSIONS OF THE CHAPTER

The changes brought by the development of new technologies have historically affected social, economic, and cultural relations. With the massive access to the Internet, rapid digitalization, enhancement of exchanges between individuals, and increase of computer processing capacity, economies in the twentieth-one century are progressively orientated towards data analysis. In the informational capitalism era, which combines informationalism as mode of development with the capitalist mode of production, platforms perform a protagonist role due to their capacity to monopolize, collect and analyze huge amounts of data. Although the word 'platform' usually refers to companies like Facebook and Google, whose profit comes mainly from advertising, it encompasses a broader universe of firms, from companies that provide the infrastructure upon which much different business will be developed to those that offer very specific services.

In this chapter, we aimed to give a brief framework of the means of operation that have made these companies the most powerful of this era. Platforms developed an impressive surveillance apparatus, through which operate guided by an extraction imperative, which states that every possible data shall be collected, even if they are not primarily related to the business. Through sophisticated mechanisms of data processing and sorting, they subsidize other businesses with information to lower their risk and increase their efficiency. On the other hand, they are constantly concerned with improving their core activity, what has been occurring through either the advances undertaken by their research and development departments or the purchase of promising startups. This leads to the creation of more varied and better quality services, attracting and retaining more users. Platforms markets, as seen, tend to suffer strong network effects, which means that the influence and prestige of a business are related to the number of their users. Markets that follow this logic tend to monopolize. As consequence, platforms are likely to acquire immense power in specific markets what gives them an impressive gatekeeping capacity in the networks they operate, controlling users' access and dictating the rules unilaterally. As we learned from the Fortnite case, the dominance of a market by few platforms may be harmful to nodes in the network, considering their tendencies to adopt

[168] ZUBOFF, op. cit.

despotic measures, denying access to the market to those who do not comply with their rules. The following flowchart summarizes the reasoning:

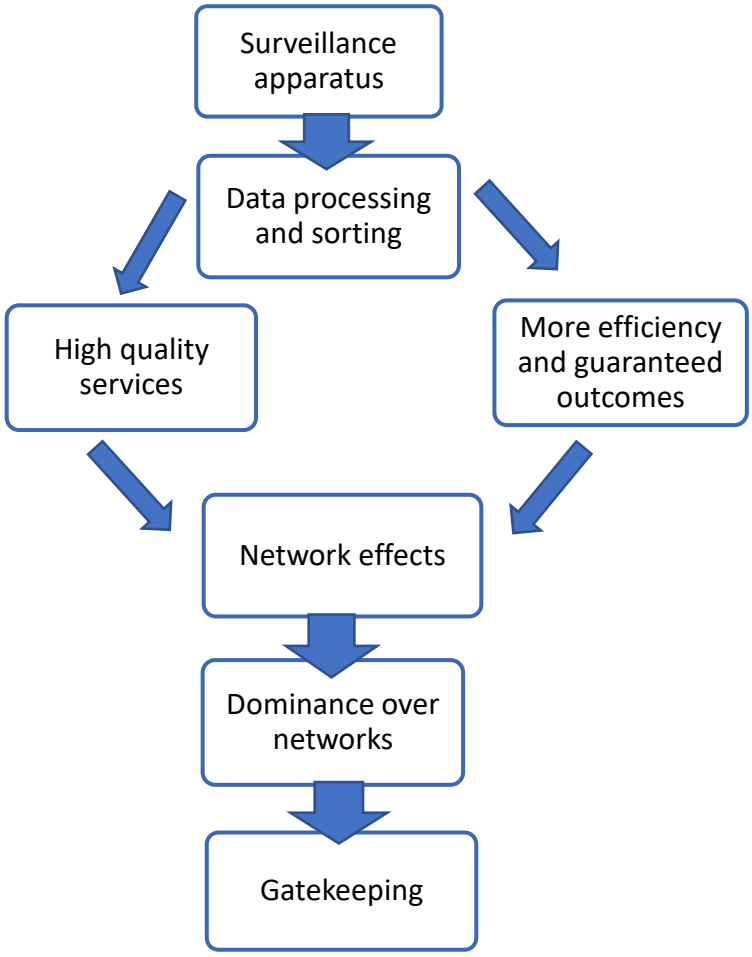

Figure 1 Relationship Between Surveillance and Gatekeeping.

Considering the centrality of data to platform businesses, these companies increasingly advance the limits of the private sphere of individuals, arising issues not only related to privacy but autonomy and self-determination.[169] Concerns related to the usage of data turned critical when the discussion surpassed the line of consumer protection and advanced to sensitive realms such as political process, as occurred in the Cambridge Analytica scandal. In order to address concerns risen from these practices, academics, regulators, and lawmakers have reflected on whether and how to regulate the potential risks derived from the increasing power of platforms

[169] ZUBOFF, op. cit.

in different aspects of public and private life they have the power to influence. This is a complex debate that involves a series of measures related to privacy, intellectual property, freedom of speech, and antitrust. The aim of this work, though, is not to cover all those subjects, but to focus on the major concerns related to consumer privacy and competition in the markets. Therefore, in the next chapters, this work intends to discuss how governmental authorities, particularly the Federal Trade Commission, are advancing those two topics.

CHAPTER 2 REGULATING ONLINE PLATFORMS: THE UNITED STATES EXPERIENCE

2.1 REGULATION IN THE AGE OF INFORMATIONAL CAPITALISM

As seen in the previous chapter, the source of productivity in informationalism lies in knowledge generation and information processing, meaning that the capacity to compete and produce efficiently depends on the generation, processing, and application of information.[170] However, informational capitalism, rather than deeply impacts the way information is generated, transmitted, and processed, has shaped broader aspects of participation of individuals in social and economic life, influencing diverse strands such as labor, financing, consumerism, and speech. In the twentieth century, the industrialization process prompted similar changes, but what makes this new mode of development unprecedented is the intermediation of those socio-economic processes by a specific type of company: the platform. Platforms' business model has its basis on the massive collection and processing of data, supported by a ubiquitous surveillance system. Concomitantly, the increasing dependence on technology grows day after day, as individuals continuously spend more time connected, with the services offered by platforms becoming especially important in our daily lives. By either functioning as large nodes in networks or even playing the role of the network itself, platforms perform a gatekeeping function, controlling, shaping, and monitoring access to information, and, consequently, how people perceive the social, economic, and cultural exchanges that are increasingly common in the online community.

Given their winner takes all tendency of some information markets, the dominance of one or few companies brings questions not only traditionally related to abuse of economic power but also the exercise of fundamental rights, raising debates about how government should respond to secure important social values, from competitiveness to democratic participation in social debates. Discussions about the viability and effectiveness of law to respond to the challenges of the informational age are not recent, though. In fact, with the popularization of Internet usage in the 1990s, digital libertarian technologists from the Silicon Valley advocated that the geography of the Internet would make it unsuitable for any form of state control, and broad access to information would revolutionize speech, public participation, and democracy.[171] By this time, regulation of the Internet was considered unfeasible and

[170] CASTELLS, op. cit., 2010, p. 77.
[171] JOHNSON; POST, op. cit.; BALKIN, Jack M., Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society, **New York University Law Review**, v. 79, n. 1, p. 1–55, 2004.

undesirable. Self-regulation by the online community would be more legitimate to respond to the then-new emerging questions.[172] This cyberlibertarian ideology found support in the United States government through the release in 1997 of the Framework for Global Electronic Commerce,[173] which embraced a pro-liberty and market-orientated vision to guide Internet policy, with maximization of free-trade and competition, through a deregulatory agenda, that persisted to dominate the following administrations. Concurrently, digital economy agenda rose in a time when government constraints to corporate abuse in realms such as antitrust and public ownership were undermined. [174] Besides, political environment - and the influences it suffers from different pressure groups - deeply inform choices about the law. Lobby from Wall Street and Silicon Valley has played a crucial role in advocating for a self-regulatory approach with the argument that technology would always be one step further than governmental oversight and that regulation would prevent innovation.[175] Platform-based industries have worked in favor of the idea that sophistication and expansion of data-processing techniques as an inevitable step further towards efficiency and economic growth, while have financed strong advocacy to target legislators, regulators and libertarians think thanks either to fight against regulations that would increase their costs and/or shape the debate around those matters.[176]

---

[172] This libertarian approach was not echoed in every realm of online activity. Authors such as Lawrence Lessig and Joel Reidenberg advocated for the necessity of regulating cyberspace. Cf. LESSIG, op. cit.; REIDENBERG, op. cit. Similarly, there was a concern about regulating online behaviors that would be harmful such as child abuse, identity fraud, and copyright infringement. As practical examples, recall that U.S. Congress enacted legislation such as the Communications Decency Act – CDA and the Digital Millennium Copyright Act – DMCA respectively in 1997 and 1998. The CDA intended to combat the circulation of pornographic material on the Internet in order to protect children, whereas the DMCA criminalized services or devices to circumvent access to copyrighted works and increased penalties for infringements that occurred on the Internet. Nonetheless, both statutes were, in fact, indulgent to Internet service providers limiting their liability for content published by users of their services, under the justification that the Internet constituted a differentiated forum for public discourse.

[173] The Framework proposed a paradigm in which "private sector should lead" Internet development, with government encouraging self-regulation whenever possible and avoiding any "undue restrictions on electronic commerce". Government should only act to foster electronic commerce and ensure competition. FRAMEWORK for Global Electronic Commerce. The White House, [s.l.] https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html

[174] STARR, Paul, How Neoliberal Policy Shaped the Internet – and What to Do About It Now. **The American Prospect,** [s.l.] Oct. 2, 2019. Available at https://prospect.org/power/how-neoliberal-policy-shaped-internet-surveillance-monopoly/. Access on Aug 18, 2020.

[175] That was exactly what Google chairman Eric Schmidt stated in the 2011 eG8 Forum that governments should not try to regulate technology, as it moves so fast that any problem would be solved by it. GOBRY, Pascal-Emmanuel. Eric Schmidt To World Leaders At eG8: Don't Regulate Us, Or Else. **Business Insider**, [s.l.] May 24, 2011. Available at https://www.businessinsider.com/eric-schmidt-google-eg8-2011-5. Access on Aug 18, 2020.

[176] MOLLA, Rani. Google, Amazon, and Facebook all spent record amounts last year lobbying the US government. **VOX**, [s.l.] Jan. 23. 2019. Available at https://www.vox.com/2019/1/23/18194328/google-amazon-facebook-lobby-record. Last access on Aug. 18, 2020; CADWALLADR, Carole; CAMPBELL, Duncan. Revealed: Facebook's global lobbying against data privacy laws. The Guardian, [s.l.] Mar. 2 2019, Available at https://www.theguardian.com/technology/2019/mar/02/facebook-global-lobbying-campaign-against-data-privacy-laws-investment. Access on Aug. 18, 2020; STOLLER, Daniel R. Facebook, Google Fund Groups Shaping Federal Privacy Debate (3). **Bloomberg Law**, [s.l.] Nov. 18, 2019,

This scenario led Zuboff to argue that both cyberlibertarian "cry for freedom" and Wall Street neoliberal agenda were the great responsible for the development of surveillance capitalism actors with no strings attached, circumventing all kinds of regulation that public authorities might subject them.[177] However, Amy Kapczynski criticizes Zuboff's argument that surveillance capitalism grew "lawless".[178] According to Kapczynski, as data is unowned, free of any property claim, Zuboff misinterprets a regulatory choice of how to deal with a certain type of information (data) with the absence of any law.[179] Such impreciseness is similar to the one that equates "deregulation" with the broad dismantling of government regulation with its substitution for a *laissez-faire* policy. Instead, deregulation may concern different regulatory approaches – e.g. privatization of public services followed by price control policies – or even to less strict obligations or enforcement.[180] Such understanding in a certain way meets the neoliberalist thought that conceives market and economic rationality not as natural, but as constructions of law and political institutions, with the state responding to the needs of the market and directing its policies towards economic rationality.[181] In this sense, deregulation relates rather to a market-orientated regulation than to the detriment of other forces in society.

Scholarship has been stressing the decisive role of law in enabling technological firms to make their business model economic viable and highly profitable.[182] In fact, surveillance infrastructures or monopolies do not appear from night today. Innovative companies that emerged in the Silicon Valley succeed in their data-driven businesses because, through the last decades, U.S. authorities in the three branches developed rules and took decisions that enabled sustainable growth of their business towards global markets.[183] Therefore, new legal regimes were created, and traditional legal concepts were subjected to a new perspective to accommodate new economic interests. Law helped platforms to grow in power through the concession of entitlements and immunities, insulating them from public oversight.[184] In this sense, the influence over the regulatory agenda is not directed towards a complete absence of

https://news.bloomberglaw.com/privacy-and-data-security/facebook-google-donate-heavily-to-privacy-advocacy-groups. Access on Aug. 18, 2020.

[177] ZUBOFF, op. cit., p. 72-78.

[178] KAPCZYNSKI, Amy. The Law of Informational Capitalism. **Yale Law Journal**, p. 1460–1515, 2020, p. 1465.

[179] Ibid., p. 1479.

[180] MAJONE, Giandomenico, Do estado positivo ao estado regulador: causas e consequências da mudança no modo de governança. **Revista Do Serviço Público**, v. 50, n. 1, p. 5-36. Available at https://doi.org/10.21874/rsp.v50i1.339. Last access on Aug. 30, 2020.

[181] BROWN, Wendy. Neo-liberalism and the end of liberal democracy. **Theory and Event**, v. 7, n. 1, 2003. Available at https://muse.jhu.edu/article/48659. Last access on Aug. 23, 2020.

[182] COHEN, op. cit., 2019; KAPCZYNSKI, op. cit.; PASQUALE, op. cit., 2015.

[183] CHANDER, Anupam. How law made Silicon Valley, **Emory Law Journal**, v. 63, n. 639, p. 639–694, 2014, p. 647-650.

[184] COHEN, op. cit., 2019, p. 104-118.

restraints, but interested restraints. Moreover, the subject of rights in certain areas, such as intellectual property and antitrust law, are powerful and organized, so the pressure to strengthen specific legal matters, whereas regulation in others, such as labor and privacy, is impaired, as the interests are diffused and disorganized.

With the advent of the Internet, technological advances permitted the replication of information at a level never seen before, posing great challenges to the enforcement of intellectual property rights.[185] With the fixation on tangible means such as books, CDs, DVDs not being necessary, the costs and time spent in copying decreased substantially and allowed sharing in a widespread fashion through individuals that were not even physically close to each other. This led to a strong reaction of different sectors in an attempt to expand property rights over data through trade secrets and copyright law.[186] Emphasis on narratives to expand intellectual property rights have its basis on production incentives, with an advantage to intermediaries – agents that provide infrastructure to authors and creators perform their work, such as industrial firms, publishers, motion picture producers.[187] In high technology markets in which platforms operate particularly, companies orient their lobby activities to protect their data processing techniques, while there is a strong lobby against regulation of access to data. The enactment of copyright statutes such as the DMCA establishes a notice and takedown regime for infringement and prevents not only circumvention of technical access protection, but also dissemination of such technical expertise, with courts making interpretations that give technology developers comprehensive control over the design and functionalities to curb management of content, even who it was lawfully acquired.[188]

Similarly, trade secrets have also been used as a justification for opacity and lower levels of access to information. But differently from copyrighted works, to which access is granted through licensing and it can even expire years after, trade secrets create a property right that does not implies disclosure of information, leaving it apart from the public domain.[189] Whereas platforms advocate for keeping access to data in the public domain, they sustain a secretive culture, contending underlying code and the means to process these data, such as machine learning techniques, and algorithms, should remain far from public oversight, and appearing as a justification to curb access of regulatory authorities to company's practices.

[185] Recall also the discussion about the expansion of intellectual property rights in section 1.1, p. 8-9.
[186] PASQUALE, op. cit., 2015; KAPCZYNSKI, op. cit..
[187] COHEN, op. cit., 2019.
[188] Ibid, p. 125-126.
[189] PASQUALE, op. cit., 2015.

If in the intellectual property realm economic interests were driven towards the expansion of a legal framework, antitrust enforcement has suffered a drawback in the last decades. Despite the existence of a solid set of federal and state statutes and common law regulating anticompetitive conducts of business corporations, as well as established federal administrative agencies in charge of enforcement - the FTC and the DOJ -, in the last decades, antitrust action in the United States was severely enfeebled, insofar as anti-concentration agenda was wiped off from the political arena.[190] The journey against antitrust law enforcement emerged in the 1970s with the theoretical support of the Chicago School of Antitrust, which advocate for a regulatory approach favorable to limited government intervention and free-market principles. Chicago School scholars defended that the main goal of antitrust law was to promote consumer welfare, through lowering prices. Antitrust law should foster efficient allocation of resources and, as result, benefit consumers through lower prices and innovative products, with markets self-correcting eventual bumps.[191] Thus, consumers' interests would be better protected when the government did not engage in interventional policies towards practices that produced an immediate benefit to consumers, meaning lower prices, even if it resulted in higher market concentration and fewer firms in the future.

Such vision influenced antitrust action in the United States, with statistics from the DOJ workload showing the decreasing of anti-monopoly enforcement and civil non-merger actions since the 1970s.[192] The decrease of antitrust action in the United States – and economic regulation through a neoliberal agenda more generally - coincides with the expansion and popularization of the Internet. Governmental guidelines towards no intervention in online businesses in the period of explosive growth of online businesses in the 1900s and early 2000s allowed the freshness of the first online entrepreneurs gave room years later to the ascension of 'big techs' who nowadays control key points of digital networks. Relying on the idea that dominance of markets does not pose a competition problem if consumer prices are low, antitrust authorities approved operations such as Microsoft's acquisition of Skype, Google's acquisition of YouTube, and Facebook's acquisition of both WhatsApp and Instagram. Certainly, communications markets are known for being more susceptible to monopolization or oligopolization due to network effects. It happened with the telegraphs between the 1840s and

[190] WU, Tim. **The curse of bigness:** antitrust in the new Gilded Age. New York: Columbia Global Reports, 2018.
[191] Cf. generally BORK, Robert. **The antitrust paradox:** a policy at war with itself. New York: Free Press, 1993. ("the whole task of antitrust can be summed up as the effort to improve allocative efficiency without impairing productive efficiency so greatly as to produce either no gain or a net loss in consumer welfare").
[192] Cf. DEPARTMENT OF JUSTICE (DOJ). **Workload Statistics**. [Washington], [between 1970-2019]. Available at https://www.justice.gov/atr/division-operations. Last visited on April 30, 2021. There is not a significant trend in DOJ's merger enforcement data.

1860s with Western Union's monopoly, with telephones between 1890s and 1910s when AT&T dominated the market, and through the 1920s, with NBC and CBS prevailed in radio.[193] However, in informational capitalism era, benchmarks from the industrial era become blurred.[194] Traditional analysis of market power relies on mechanisms such as the price of a product or services and costs of entry but the assessment of platforms market power proves to be challenging, so courts and regulatory authorities must take into account the effects in all sides of the platforms, as they have interdependent demands. [195]

Platforms operate in two or multi-sided markets, in which usually service is offered free or subsidized price to one side,[196] and recover their losses in the other one, with the platform functioning as a bridge between the two or more sides. Therefore, there may be no anticompetitive conduct in course, as users have access to high-quality services without having to pay or paying a small amount, and can freely move from a service to another if they are dissatisfied with the quality of the service offered, but this reasoning is misleading. Firstly, assessment of market power over consumers' side should not be grounded on the platform capacity to increase the price of the service, but on whether a decrease in the quality of the service would lead users to migrate to other online services, whether they cannot migrate to another one or it would come at a high cost.[197]Secondly, to get a full picture, it is necessary to look at all sides of the business. If there are a myriad of options available for users, it may be not true for advertisers, who can endure very high prices for their products appear on the most used platforms. For instance, Facebook and Google dominate the digital advertisement market[198] and Amazon alone is responsible for almost half of the market share of the U.S. e-commerce retail market.[199] Thirdly, although platform services are offered free, it does not mean that they are costless, as the platform business model relies on heavy collection of data, so even when a given service is offered at zero cost, users are in fact exchanging them for their personal data.[200] The metadata generated constitutes a valuable resource sold in markets of

[193] STARR, op. cit.
[194] COHEN, op. cit., 2019, p. 173.
[195] EVANS, op. cit.
[196] FRIEDEN, Rob. The Internet of platforms and two-sided markets: implications for competition and consumers. **Villanova Law Review**, v. 63, n. 2, p. 269–320, 2018.
[197] EVANS, op. cit., p. 26.
[198] REYES, Mariel Soto. Google, Facebook, and Amazon will account for nearly two-thirds of total US digital ad spending this year. **Business Insider**, [s.l.] Dec. 3 2020. Available at https://www.businessinsider.com/google-facebook-amazon-were-biggest-ad-revenue-winners-this-year-2020-12. Access on May 15, 2021.
[199] DROESCH, Blake. Amazon dominates US commerce though its market share varies by category. **Emarketer**, [s.l.], April 27 2021. Available at https://www.emarketer.com/content/amazon-dominates-us-ecommerce-though-its-market-share-varies-by-category. Access on May 15, 2021.
[200] FRIEDEN, op. cit; COHEN, op. cit.

future behavior. One may argue that the interdependence of markets and the ability of platforms to connect them are what make them valuable, so, as they must keep continuously offering high quality and innovative services to keep themselves relevant, there is a positive effect on consumers' welfare to remain competitive.[201] This is partly true, considering that one of the main goals of advertisement-based platforms is to hold users' attention and foment addictive behaviors so they spend a significant amount of time in the network. Platforms must develop means and give incentives to grab the attention of their users so that they can extract massive amounts of data.

Besides, new players may face barriers to entry into the platform market. Despite the Silicon Valley narrative that disruptive services are daily emerging in technology markets, as companies do not need to endure heavy infrastructure and supply costs in their installation and operate in high levels of economies of scale, big techs are nowadays closer to oligopolistic firms such as Microsoft and AT&T than fresh startups. As platforms serve as points of connection of interdependent markets, one side of the markets will only adhere to the service if the other do so (indirect network effect). This can be particularly challenging because it implies new entrants reside modifying users' habits. As platform services are experience goods,[202] non-users tend to give a trial to strong and well-established brands and users face high switching costs, benefiting market leader firms. [203] In informational capitalism, data is a key asset, so well-established platforms with great access to data have competitive advantages, as the more information they can harvest, the better they will develop algorithms and AI processes and get better outcomes to both offers in markets of future behavior and enhance their services, and thus enlarge their markets, in a virtuous cycle. This is especially true for big technology companies that operate in vertically integrated markets and are capable of collecting massive quantities and quality data. Thus, new entrants in digital markets may face barriers to have access to databases, which may leave them in a disadvantaged position. On the other hand, it is undeniable that the services provided by platforms are nonrivalrous, which means that an unlimited number of users can access them and simultaneously to other similar ones. An Instagram user is not impeded to have a TikTok account or watch videos on YouTube. In practical terms, it may be difficult to prove that certain service has a dominant position because it imposes barriers to entry.

[201] FRIEDEN, op. cit., p. 278.
[202] Experience goods or services refer to those whose quality or price is difficult to evaluate in advance, consumers need to test them to have an opinion.
[203] BARWISE; WATKINS, op. cit., p. 25.

Big tech companies are definitely efficient in delivering personalized and fine-tuning digital applications that are constantly updated with new functionalities. Their willingness to innovate is more related to a search for new methods to extract personal data, find new patterns of behavior and profit opportunities. It could be argued that, as platforms' business model relies on attention seek of users, there is a dynamic competition to offer the best, so if platforms do not equally engage in offering more privacy protection for their users, privacy probably is not a priority, as they keep choosing privacy-invasive series such as Gmail and Facebook. However, users have a low level of understanding of profiling techniques undertaken by intermediaries. Besides, due to network effects, one would argue that incumbent platforms do not face competition to offer more or less privacy to users, as just a few companies concentrate high traffic of information flows and outstanding processing capacity, which grants little choice to those searching for privacy-friendly options. "Without entry or the credible threat of entry, digital platforms need not work hard to serve consumers because they do not risk losing their consumers to a rival."[204]

The influence of Chicago School doctrine over bureaucracy and political arena, allied with practical difficulties to analyze antitrust claims in digital markets presents a challenge to enforcement authorities, and allowed a significant market concentration in the hands of few companies, particularly through the approval of mergers. Lack of competition in digital markets and accumulation of data in the hands of few companies causes not only economic harms but also social harms associated with loss of privacy and even political harms, derived from their power over information (and misinformation) dissemination, leading to reflection about the role and goals of antitrust enforcement, with the protection of non-economic values, such as privacy and free speech.[205]

On the other hand, the interests of large populations that have been enduring the negative effects of informationalism remain uncovered or not fully contemplated by legal institutions. In the matter of privacy, the question that emerges is whether and what kind of response scholarship and governmental authorities can offer to ubiquitous surveillance and the harms that may derive from constant exposure. With the growth of the Internet, despite the concerns related to information disclosure online, there was persistent concern about the enactment of a

[204] ZINGALES, Luigi; ROLNIK, Guy; LANCIER, Filippo Maria (Orgs.). **Stigler committee on digital platforms, Final Report**. [Chicago], September 2019. Available at https://research.chicagobooth.edu/stigler/media/news/committee-on-digitalplatforms-final-report. Last access on May 3, 2021, p. 43.

[205] FUKUYAMA, Francis *et al*. **Report of the working group on platform scale.** Stanford: [s.n.], 2020. Available at https://cyber.fsi.stanford.edu/publication/report-working-group-platform-scale. Last access on Jan. 3, 2021.

strong and comprehensive regulation that would curb technological advances. In the European Union and Latin American countries, such as Argentina, Brazil, and Chile, there has been recognized a data protection right. In the European Union, specifically, with the Data Protection Directive 95/46/EC and especially after the enactment of the GDPR, regulatory authorities have recognized data protection as a new fundamental right set out in Article 8 of the EU Charter of Fundamental Rights.

In the United States, protection against intrusive data collection emerges as a dimension of the right to privacy, insofar as technological changes in society lead privacy law to grow thicker. American information privacy debate has been historically influenced by the idea of privacy as control over information,[206] under which "policy should empower individuals to make informed decisions about the collection and use of personal information".[207] This conception of privacy inspired the FTC to adopt the so-called Fair Information Practice Principles (FIPPs), guidelines developed by the US Department of Health and Education for online companies to provide adequate privacy protection in the electronic marketplace, which later inspired the Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[208] Although those principles do not carry the force of law, they have had a persuasive character and orientated regulatory oversight. The core principles listed in the FIPPs are notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress. Notice and choice principles in particular favored the adoption by the Commission of a "notice and choice" approach, which relied on consumers' self-awareness and clear notice about the information being collected and on their free choice to accept or not the privacy policies imposed by websites. The idea was to make collection practices more transparent and provide users with the necessary tools to have control over their information, without a strong regulatory interference over what kind of information and in which circumstances it could be collected and processed. Despite FTC's recommendations, US Congress did not pass any statute requiring

[206] In the United States, theory of privacy encompasses different conceptions. Warren and Brandeis's traditional conception of privacy refers to a "right to be let alone", whereas other theorists conceptualize privacy as "limited access to the self" or "secrecy of certain matters". Other theories understand privacy as "a form of intimacy" or "a form of protecting personhood". Cf. SOLOVE, Daniel J. **Understanding privacy**, Cambridge: Harvard University Press, 2008, p. 14 and ss.

[207] HOOFNAGLE, Chris Jay. **Federal Trade Commission privacy law and policy**. New York: Cambridge University Press, 2016, p. 148.

[208] For more information about the OECD Guidelines, Cf. BAUMER, David L.; EARP, Julia B.; POINTDEXTER, J. C. Internet privacy law: a comparison between the United States and the European Union. **Computers & Security**, p. 400–412, 2004.

businesses to comply with FIIPs.[209] Thus, as will be seen in subsection 2.3.1, the FTC encouraged self-regulation, with the first cases on information privacy having their basis on the broken promises of privacy, in which the Commission acted to enforce privacy policies of websites through Section 5 enforcement on deceptive practices. However, this approach has proven insufficient to address current privacy challenges.

Concerns about the incursion of private firms over personal data freely available for appropriation grew with the increasing popularization of the Internet. Relying on the idea of privacy as control over information, some theorists, in the first decade of the twentieth century, discussed whether it should be recognized as a property right on data.[210] The conception of personal information as property has its grounds on the idea that an individual's property is an extension of his or her personality.[211] Although it seemed intuitively a good response to address the issue of personal data as public domain, this approach hardly addressed or mitigated the questions that arose with the emergence of the online platform. To illustrate this point, consider the discussion about control over information, which is not recent,[212] but acquired new contours with the debate around the regulation of data collection. Departing from a romantic idea of authorship embraced by the Supreme Court of California in *Moore v. Regents of the University of California*,[213] data-driven companies have vindicated the conception of personal data as raw

[209] SERWIN, Andrew B. The Federal Trade Commission and privacy: defining enforcement and encouraging the adoption of best practices. **San Diego Law Review**, v. 48, n. 809, p. 809–856, 2011.

[210] Cf. LESSIG, op. cit. (defending the use of property rights as a mean to control information on the Internet); LITMAN, Jessica. Information privacy / information property. **Stanford Law Review**, v. 52, n. 5, p. 1283–1313, 2000 (arguing that a property right over personal information is unlikely to succeed); SCHWARTZ, Paul M. Property, privacy, and personal data. **Harvard Law Review**, v. 117, n. 7, p. 2056–2128, 2004 (advocating for a model of propertization of personal information sensitive to potential threats to personal privacy).

[211] SOLOVE, op. cit., 2008, p. 26.

[212] In a letter to Isaac McPherson in 1813, Thomas Jefferson stated that "*if nature has made one thing less susceptible than all others of exclusive property, it is the action of the thinking power called an idea"*. While vacillating about the conception of property as a natural right, Jefferson considered that the exclusive right to an invention was not encompassed by this notion but should be granted for the benefit of society. An idea indeed has ethereal character, as it can be kept in our heads or freely flow in exchanges with other people. Communication of thoughts, ideas, beliefs is inherently humane and is not something over any government that may have total control, even in the toughest state of exception. Thomas Jefferson to Isaac McPherson, 13 August 1813," **Founders Online**, National Archives, https://founders.archives.gov/documents/Jefferson/03-06-02-0322.

[213] UNITED STATES. Supreme Court. Moore v. Regents of University of California, 51 Cal. 3d 120 (1990). First party: John Moore. Second-party: The Regents of the University of California *et al.* Jul. 9, 1990. Available at https://law.justia.com/cases/california/supreme-court/3d/51/120.html. Access on: Mar. 3, 2021. John Moore was a patient at UCLA Medical Center treating leukemia. His physician, David Golde, took samples of Moore's blood, spleen cells, bone marrow, and other bodily substances. Golde managed to establish a cell line using Moore's cells and patented it. Moore filed an action claiming property rights over his bodily tissues that made possible Golde's research, patent, and commercial exploration of the results. The Supreme Court of California rejected the argument that one has property rights over his body tissues as his cells, used as raw materials to create the patented cell line, were not more unique than any other person. Human cell lines are patentable and thus capable of generating a property right, because of the inventive effort in its fabrication. Besides, the recognition of Moore's property rights over the cells of his own body would impose a duty on scientists that would burden medical research that is essential to all society.

material freely available for appropriation. The *Moore* court concluded that his property claims over his cells and body fluids were too limited, and did not illustrate any creative effort of his part, while it would represent if legally accepted, an incursion towards privatization of public domain and inhibit of scientific research; the UCLA researchers, on the other hand, would be entitled to intellectual property rights due to their inventive labor to create cell lines.[214]

Just as in Moore's reasoning, data-driven companies have advocated for legal constructions in which personal data resides in the public domain, but information derived from algorithmic analysis and massive computer power themselves shall be protected through intellectual property regime, either as patented good or trade secret, naturalizing surveillance techniques for data collection, whereas data as mere raw material shall be left in the public domain.[215] As seen in the first chapter, the exponential growth of computer capacity to process data through complex algorithms has made feasible the production of meaningful information that will turn into valuable corporate assets. In this sense, those who have access to large amounts of data and expertise to manage it have a considerable advantage when making decisions and designing strategies. Thus, access to data also involves the distribution of wealth and power, but only to specific actors involved in this process, the twentieth-first century bourgeoisie that does not own the means of production but the means of processing.

The idea of granting property rights to control access to personal data, and then safeguard the right to privacy on the Internet departs from a Lockean conception of property as a natural right and the commodification of information on the Internet, in which data is a valuable good that will be the foundation of informational economy chain of value.[216] Besides, the idea of propertization of personal data would furnish a market-based response to privacy interests over data without relying on any kind of governmental intrusion in this field.[217] If data is becoming such a valuable asset, why do not grant an economic advantage to those willing to sell them to private companies? Although, at glance, it seems a reasonable response to assert user's privacy rights, granting them a choice on whether or not to sell their information and, then, economic advantage for the sale, such regime would have to face questions related legal challenges related to the concept of property and transmission of information. Additionally, in

[214] BOYLE, op. cit, 1992, p. 1519.
[215] COHEN, op. cit, 2019, p.71-73.
[216] SOLOVE, op. cit, 2008, p. 25-26.
[217] LITMAN, op. cit, p. 1293 ("If ownership of private property is power, however, calling privacy rights "property rights" offers the promise of magically vesting the powerless with control over their personal data. Because the law of private property is perceived as a-regulatory, this approach seems to answer the objections raised against significant government regulation").

the end, property rights over information would reveal themselves as an undesirable incursion considering the basis of the platform business model.

Legal challenges to conceive information privacy as property of personal data lie in the efforts to translate property rights to the context of the online world, such as alienability and secondary use. In the real world, usually, there is neither restriction on the sale or exchange of any good nor restrictions on the buyer's rights to resell the good. The exceptions are narrowly tailored by law and address social and economic values dear to society. Thus, to avoid the free circulation of users' data and protect privacy commons, it would be necessary to design a regime of inalienability.[218] The creation of such a regime, however, is not simple, as implies the creation of mechanisms to enforce it. Recalling the 'pathetic dot' model conceived by Lessig, the property is subject to a set of different protections of law, norms, market, and architecture.[219] In 'real-world', property can be protected by real-space code (fences, locks), whenever law is not enough, whereas law itself is required when the other three modalities fail to safeguard property.[220] In the online world, unawareness about collection of data turns private measures more complex, thus, probably a certain degree of governmental monitoring and enforcement mechanisms would be necessary. Besides, personal information is often formed through relationships with others, web-browsing information derives from interactions between users and websites and not from the lonely work of individuals.[221]

Most importantly, granting property rights on personal data would not affect the grounds of the platform business model and would have the potential to create undesirable secondary effects. Consumers access search engine results, create accounts on a social network, or listen to their favorite songs through streaming without any additional cost, while sellers spent a lot of money to target those individuals online. The apparent costless provision of such services reveals as a barter system in which users exchange their data of access to those services. Thus, even if personal data would be treated as property, access to any kind of service or content would be conditioned to transference by agreeing with the terms of clickwrap contracts. Considering the gatekeeping function exerted by platforms, in a scenario of market concentration, consumers hardly will have sufficient power to negotiate equally a fair price with platforms. On the other hand, due to network effects, users are increasingly dependent on certain platform services.

[218] SCHWARTZ, op. cit.
[219] LESSIG, op. cit, p. 171.
[220] Id.
[221] SOLOVE, op. cit, p. 27.

Indeed, not all juridical relationships should be seen through the lens of market transactions, especially when it comes to the enjoyment of fundamental rights. Returning to *Moore's* case, although the Californian court did not recognize the right to property over bodily tissues, it did not leave Mr. Moore completely neglected, as the judges recognized that, as a consumer, Moore was entitled with the right to make informed decisions. Similarly, when it comes to platform business models, although users are not granted ownership over their personal data, it does not mean resistance to data collection as well as the vindication of legal policies to address the potential dangers of ubiquitous surveillance is not viable through other approaches.

Conceptions of information privacy as control over information depart from an individual-focused paradigm that seems insufficient to address the potential harms of mass surveillance. Such conception of privacy leads to structural difficulties in defining what is meant by "control", especially when control lead to a clash with other constitutionally protected rights, such as free speech, high compelling governmental interests, such as national security, or social pursued values, such as innovation and efficiency. Moreover, ubiquitous surveillance undertaken in hyper-connected times brings additional difficulties to privacy protection frameworks that rely predominantly on users' choices on disclosure of information. This is because, despite the orientation towards user awareness to allow informed consent for them to determine the level of access to their information, the relationship is still asymmetric. The complexity of the data-cycle of personal data processing and the difficulty to recognize potential harms derived from data collection, aggregation, and processing possibilities prevent individuals to have a precise view of the consequences of their choices, recognize the nexus between choices and injury, and articulate resistance. This is because although privacy harms are more apparent when they involve insult and economic damage, they also derive from technological architecture, leading to more systemic problems.

Information technologies, such as platform services, are increasingly intermediating social interactions. Debates regarding equality, freedom, political and economic structures, social behaviors, and so forth historically have been present in the public arena. The popularization of the Internet, in special networks that enabled the democratization of content creation, like social media or messenger apps, allowed social groups that had no voice in traditional media vehicles had the unprecedented opportunity to echo their voices – for the good

and the bad.[222] However, as already argued, technology is not neutral. Architectural choices related to the data collection, automated decisions driven by algorithms, profiling techniques, and even interface design have demonstrated capable of modifying the perception of the world in a fashion that is not apparent for ordinary users.[223] Information technologies have the potential to influence not only individuals' behavior as consumers in the marketplace but also the exercise of citizenship.[224]

In this sense, Zuboff argues that surveillance capitalism reveals as a threat to human autonomy, as it moves towards behavioral modification of individuals. Taking as example Pokémon Go and Facebook news feed experiments, she argues that through a variety of processes, techniques, and tactics, platforms are shaping populations' behavior to guarantee financial outcomes, and developing what she defines as an 'instrumentarian power'.[225] It consists of a new form of power in which surveillance apparatus – the Big Other – extracts behavioral surplus to recognize patterns of behavior and resorts to means of behavioral modification to guarantee outcomes.[226] Although recognizing the importance of Zuboff's work in describing data manipulation cycle, Amy Kapczynski argues that concerns related to target advertising and threats to individual autonomy should not be regarded as central in the context of informational capitalism, as there are more urgent and bigger problems to be faced, such as platform power, impact on labor and monopolization tendencies.[227] Indeed, target advertising may have a limited effect on users' behavior, but it is not totally clear the extent to which digital platforms, through techniques most of the time obscure to users, intervene in users' behavior towards specific directions. Some experiments raise concerns, such as the one undertaken by Facebook in May 2012 when it allowed users to disclose their organ donor status, leading to a boost on organ donor registration, or when it allowed users to update their profile with an "I voted" button, what drove an increase of 340,000 voters in the 2010 midterm elections.[228] Had

[222] As an example, think about how Twitter has been used by organized groups in a coordinated fashion, for instance through the usage of the same hashtag, to raise awareness for a topic.
[223] COHEN, op. cit, 2012, p. 129-132.
[224] Id.
[225] ZUBOFF, op. cit, p. 237-239.
[226] ZUBOFF, op. cit, p. 237-239.
[227] KAPCZYNSKI, op. cit, p. 1460.
[228] THE FACEBOOK effect: social media dramatically boosts organ donor registration**. John Hopkins Medicine**, [s.l.], June 18, 2013. Available at https://www.hopkinsmedicine.org/news/media/releases/the_facebook_effect_social_media_dramatically_boosts_organ_donor_registration. Last access on Apr. 12, 2021; LIND, Data. Facebook "I voted" sticker was a secret experiment on its users, **Vox** Nov 4, 2014. Available at https://www.vox.com/2014/11/4/7154641/midterm-elections-2014-voted-facebook-friends-vote-polls. Access on Apr. 12, 2021.

Facebook mapped the political preferences of users in a given state, it could nudge those with a specific political orientation to go vote according to the company's interest.

The ability of these information technologies to record, aggregate make inferences and suggestions through a vast amount of data enable reconstruction of the individual activities beyond what a person would expect. Such information asymmetry increases the power of governments and companies over individuals, allowing them to make decisions about them and modulating behavior, through practices with potentially harmful impacts on democracy and autonomy.[229] On the other hand, pervasive surveillance can cause a chilling effect on speech and other activities, leading to inhibition, as a certain degree of concealment is necessary for individual critical thought to flourish.[230]

Therefore, the right to privacy should no longer be regarded solely as an individual right, centered on the decision of which data is accessible or not, but as a collective right, because the risks associated with mass surveillance surpass the individual's subjectivity and individuals have a very narrow view of the likelihood and consequences of potential damages, being hardly perceived when not observed in the broad scenario. [231] As consequence, democratic citizenship and human autonomy should be taken into account as underpinnings in the construction of the privacy regulation debate.[232] The difficulty here lies in the regulatory design to concrete this collective dimension of privacy. In industrial capitalism, the regulatory state emerged as a response to the risks to public health and safety through the establishment of administrative agencies and the enactment of regulation over economic sectors. Comparatively, in the informational capitalism era, the risks associated with information-based processes are more subtle, and classical regulatory tools such as rulemaking and adjudication have their efficacy questioned.

It has been long discussed whether and how the privacy framework in the United States should be adjusted to contemplate those new challenges derived from the informational

[229] According to Zuboff, surveillance capitalists shape individuals' behavior through processes she calls "economies of actions". She identifies three key approaches: tuning, herding, and conditioning. ZUBOFF, op. cit., p. 132-133; Cf. COHEN, Julie E., What privacy is for, **Harvard Law Review**, v. 126, n. 7, p. 1904–1933, p. 1912 2013 ("A society that permits the unchecked ascendancy of surveillance infrastructures cannot hope to remain a liberal democracy"); MOROZOV, Evgeny, The real privacy problem, **MIT Technology Review**, v. 118, n. 8, p. 33–43, 2013 (arguing that privacy is a mean to democracy, not an end in itself).

[230] SOLOVE, Daniel J., A taxonomy of privacy, **University of Pennsylvania Law Review**, v. 154, n. 3, p. 477–560, 2006, p. 487; COHEN, op. cit., 2013.

[231] ACQUISTI, Alessandro; GROSSKLAGS, Jens, What can behavioral economics teach us about privacy?, **Digital Privacy: Theory, Technologies, and Practices**, p. 363–377, 2007, p. 367 ("An individual who is facing privacy-sensitive scenarios may be uncertain about the values of possible outcomes and their probability of occurrence and that sometimes she may not be able to form any beliefs about those values and those possibilities").

[232] COHEN, op. cit., 2013.

economy. As seen in this section, the United States took a different path from European Union and other countries in the world and has not enacted, until now at least, a general statute to regulate personal data flow. Nor it has created an independent governmental agency to address privacy-related topics. However, it does not mean that the country has not made any progress in this realm. Apart from some sectorial statutes focused on a specific type of information, the United States, at the federal level, has been developing a privacy regulatory framework through the FTC decisions on enforcement cases, with its broad authority to protect consumers in different economic sectors. Thus, given the protagonist character the FTC acquire in the privacy debate over the last two decades, a debate around the regulation of platform surveillance must necessarily pass through the Commissions' performance.

On the other hand, as seen in the first chapter, there is a relationship between surveillance practices and gatekeeping power deployed by platforms. Such capacity to influence information flows derives from the omnipresence of big techs in the online space and the growing dependence on their services, given their dominance on different digital markets. As surveillance intertwines with gatekeeping, effective regulation of platforms can only be fully addressed when targets the two sides of the coin. The FTC is also responsible for the regulation of anti-competitive practices, with the authority to fight against acts or practices in violation of antitrust law and undertake pre-merger analysis. This dualistic mandate to enforce actions against violation of privacy and competition positions the Commission in a privileged spot to address the risks posed by digital platforms. However, to have a better understanding of the FTC authority, its limitations, and challenges in the American federal administrative structure, the next section will present a brief explanation of regulatory agencies' structure and the procedural forms of administrative action.

2.2 A FRAMEWORK OF INDEPENDENT AGENCIES IN THE UNITED STATES

The first decades of the twentieth-first century were marked by an accelerated transition from a traditional industrial society to an informational one, characterized by the exponential increase of data flows and the development of business models based on the production, accumulation, and processing of information. If this shift from atoms to bits[233] contribute to the spreading of various types of content and connected people as never before, it has also

[233] MURRAY, op. cit., 2013. ("In the information society we see a shift from encoding information in atoms (such as writing it on a page) to encoding in bits (such as word processing it). But this move is not limited to the written word: it may be sounds, images, or electrical outputs. Almost everything which may be recorded may be digitized").

represented a challenge in terms of regulation of privacy, copyright, security, and so forth. Throughout the end of the nineteenth century and the beginning of the twentieth century, social-economic phenomena such as industrialization, urbanization, and mass consumption lead to the creation of a complex net of relationships between individuals and firms. Changes in communications, means of transportation, and markets implicated the rise of many private companies as powerful actors in some markets as well as the creation of new risks for society. On the other hand, despite consumers' demands, industries responsible for the fabrication of new products eventually did not want to internalize the risks created or invest in processes to decrease them. As consequence, many disputes ended up in Courts, with judges ruling on liability due to defective products [234] or negligent labeling. [235] Until then, common law, especially torts and contract law, was the main source of regulation of economic power. Nonetheless, problems of "inequality of weapons" between large corporations and small businesses or consumers lighted in the American society a sense of injustice, also fed by narratives of bribery and political influence in the selection of judges.[236]

The rise of the regulatory state represented a shift in the relationship between private individuals and companies. In this new paradigm, the State acquires an active role in the enactment of policies and in the coordination of private activities considered either critical social interest (*e.g.* electricity distribution, telecommunications) or sensitive to safety and health of the general public (*e.g.* environmental damages, labor injuries, food safety), especially through the enactment of sectorial legislation and the creation of specialized agencies. According to Glaeser and Shleifer, three efficiency arguments favor the prevalence of regulation over litigation.[237] Firstly, regulators have technical skills comparing to generalist judges. Thus, because they are specialists, regulators are in a better position to investigate private actors and gather information. Secondly, regulators play an important role in simplifying the regulatory processes. It can occur in different ways. Different actors' interests can be represented in the regulatory process, which implies more pluralist decisions, and the regulator itself can bring an action before the court itself, which can function as a collective action and

[234] UNITED STATES. NY Court of Appeals. MacPherson v. Buick Motor Co., 217 N.Y. 382, 111 N.E. 1050. (1916) First party: Donald C. MacPherson; Second party: Buick Motor Company. March 14, 1916. Available at http://www.courts.state.ny.us/reporter/archives/macpherson_buick.htm. Last access on Nov 9, 2020.
[235] UNITED STATES. NY Court of Appeals. Thomas v. Winchester, 6 N.Y. 397 (1852). First party: Thomas and wife. Second-party: Winchester. July 1852. Available at http://www.courts.state.ny.us/reporter/archives/thomas_winchester.htm. Last access on Nov. 9, 2020.
[236] GLAESER, Edward L.; SHLEIFER, Andrei, The Rise of the Regulatory State, **Journal of Economic Literature**, v. 41, p. 401–425, 2003, p. 405-407.
[237] *Ibid*.

lead to the analysis of small-value damages that otherwise would not be claimed. Thirdly, courts' action occurs on a retrospective sight, as when they announce a new rule, it applies to prior conducts of the parties, which can bring a degree of legal uncertainty. Courts are also inherently reactive to issues emerging in society, whereas regulators can work in advance over them to prevent the occurrence of an injury at a cheaper cost. These problems led common law adjudication to be perceived as an inadequate mechanism of regulation of markets to address the new social and economic conflicts erupting in American society.

In this context, the Legislative Branch, elected by the people, plays an important role in calling different segments of society to discuss, through participation in the legislative process, what kind of risks and activities deserve state intervention. In this process, different social actors may intervene to help legislators electing what values are important to that society and shall be protected through regulation, what Cass Sunstein defined as 'pre-commitments'.[238] The existence of a regulation that reflects these social values is essential for people to have faith in the political process and feel represented in it, for the consubstantiation of these pre-commitments in statutes serves as an important protection of those values from eventual legislative majorities that might not reflect them. It does not mean, however, that this relationship between congressional representatives and the people is exempted from problems. As the larger part of the population is politically disorganized, they do not engage substantially in the political process, whereas small and well-organized groups have their claims heard more often, as they have political and economic mechanisms to influence in the legislative process, what can become problematic in terms of the democratic process, as legislators agenda may not reflect people's will.[239]

On the other hand, there is the principal-agent problem. Legislators do face this expertise problem. Thus, in order to address the pre-commitments pivotal to the people, Congress delegates substantive power to administrative agencies. As Terry Moe explains, with the growing complexity of social and economic demands, having the political power to address them is not enough, there must have the knowledge to create effective policies.[240] To solve this problem, congressional representatives write general norms and delegate broad authority to the

[238] Cf. SUNSTEIN, Cass, **After the Rights Revolution: Reconceiving the Regulatory State**, Cambridge: Harvard University Press, 1993.
[239] Cf. Mancur Olson. **The Logic of Collective Action**. Cambridge, Mass: Harvard University Press, 1965.
[240] MOE, Terry M. The Politics of Bureaucratic Structure. *In*: CHUBB, John E.; PETERSON, Paul E. (Orgs.), **Can the Government Govern?**, Washington: The Brookings Institution, 1989, p. 267–329, p. 270.

bureaucracy in administrative agencies, which have specialization and technicality to comply with their goals, fill eventual gaps and make whatever adjustment that might be needed.[241]

Administrative agencies are divided into two categories: executive-branch agencies and independent agencies. Both types of agencies have their heads appointed by the President with advice and consent of the Senate. However, Executive-branch agencies appear under the President of the United States in governmental structure and are usually ruled by a single person and can be fired at will,[242] whereas independent agencies are generally ruled by a multimember commission or board with specialized mandates. In the latter, there are restrictions on the presidential removal power, as their heads can only be removed for cause. Independent agencies occupy a unique role in the American administrative system, because they are, as their nomenclature suggests, independent of the executive branch, placed beyond the presidential sphere of direct interference. However, although they may have broad rulemaking authority as well as power to conduct adjudicative hearings and investigations, they are neither part of the Judiciary nor the Legislative branch. Despite the difficulty to fit them in the tripartite structure of government brought by the US Constitution, the Supreme Court upheld their constitutionality.[243]

Nevertheless, they must not lose control over agencies' actions, there is a risk of agencies pursue the own goals of their staff rather than from the Legislative branch, as these experts also have their own interests, and technicality of some themes may turn political oversight difficult.[244] Thus, to curb this risk, the owners of political power create procedures to orientate the decision-making process and evaluate staff's performance, require reports and information about internal operations, and settle oversight procedures.[245] Because of that, the agency decision-making process is subject to a series of procedural requirements, imposed not only generally by the constitutional clause of due process, but also by the Federal Administrative

[241]Ibid., p. 271-272.
[242] Cf. UNITED STATES. Supreme Court. Myers v. United States, 272 US 52 (1925), in which the Supreme Court ruled that the U.S. Constitution grants the President the sole power to remove executive officers under the Vesting Clause (Article 1, Section 1, clause 1).
[243] Cf. UNITED STATES. Supreme Court. Humphrey's Executor v. United States, 295 U.S. 602 (1935). May 27, 1935. Available at https://supreme.justia.com/cases/federal/us/295/602/; UNITED STATES. Supreme Court. Wiener v. United States, 357 U.S. 349 (1958). June 30, 1958. Available at https://supreme.justia.com/cases/federal/us/357/349/. In Humphrey's Executor, the Supreme Court distinguished it from *Myers*, for considering that removal powers depend on the nature of the office, and the Federal Trade Commission acts quasi-legislatively and quasi-judicially in administering the provisions of its statute. In *Weiner*, the Supreme Court held that Congress had the authority to create bodies free from control or coercive influence of either the Executive or the Congress. Giving the "intrinsic judicial character" of the War Claim Commission's activities, it was required that it could adjudicate claims free from any kind of Executive pressure.
[244] Id.
[245] Id.

Procedure Act (APA)[246] and specific sectorial statutes that define agency structure, their competences, and specific standards to guide their action. However, it does not mean that the Legislative Branch is the only one to shape agency action. Indeed, since the enactment of the APA, judicial decisions have deeply informed agencies' decision-making process, either expanding or restricting administrative procedural requirements, or defining the scope of judicial review.[247] Similarly, the Executive Branch also has its political instruments to drive through the requisition of regulatory plans and impact analysis.[248]

The APA prescribes the general rules applied to federal administration, dividing agency action into two main categories, rulemaking, and adjudication, establish standards for judicial review, regulates information disclosure to the public through the Freedom of Information Act (FOIA) amendments, and defines procedures to staff selection. Through rulemaking process, administrative agencies enact regulations that complement and specify statutes enacted by the Legislative Branch, adding more technical and scientific expertise to a given policy. The APA establishes two rulemaking procedures: informal and formal rulemaking. [249] Informal rulemaking, as known as 'notice and comment' procedure, is depicted in §§553 of the Act, which describes the minimum requirements for a regulation proposal to be adopted as a rule. The notice-and-comment procedure follows three phases: notice, comment, and publication. The general notice, published at the Federal Register, is considered flexible as it may contain "either the terms or substance of the proposed rule or a description of the subjects and issues involved".[250] In the second phase – comment - public participation occurs through written submissions of interested parties that will be taken into consideration by the agency staff during the final draft of the rule.[251] In the third phase – publication – the agency publishes the final rule followed by a justification of the regulatory choices made by the staff.

On the other hand, the agency must follow formal rulemaking when its statute requires rulemaking "to be made on the record after opportunity for an agency hearing".[252] In this case,

---

[246] UNITED STATES. UNITED STATES CODE (USC). Title 5. Ch. 5, Subchapter II §551-59, Administrative Procedure Act (APA). Available at https://www.law.cornell.edu/uscode/text/5/part-I/chapter-5/subchapter-II.

[247] Cf., for instance, UNITED STATES. Supreme Court. Vermont Yankee Nuclear Power Corp. v. Natural Resources Defense Council, 435 U.S. 519 (1978). Apr. 3, 1978. Available at https://supreme.justia.com/cases/federal/us/435/519/;UNITED STATES. Supreme Court. Motor Vehicle Manufacturers Association of the United States, Inc. v. State Farm Mutual Automobile Insurance Company, 463 U.S. 29 (1983), June 24, 1983. Available at https://supreme.justia.com/cases/federal/us/463/29/.

[248] STRAUSS, Peter L. **Administrative Justice in the United States**. Third edit. Durham: Carolina Academic Press, 2016, p. 144.

[249] Although the APA does not mention it expressly, some agencies adopt hybrid, which blends elements of both formal and informal rulemaking.

[250] APA §553 (b) (3).

[251] APA §553 (c).

[252] Ibid.

the agency must observe rules about hearings, evidence, and decision-making carved in §§556-557 of the APA, which resembles those of adjudicatory processes.[253] Given its burdensome character, formal rulemaking is the least adopted procedure, with agencies embracing it only when their statute expressly requires rulemaking to be conducted “on the record". Thus, whenever possible, most of the agencies tend to follow notice-and-comment to create and amend their administrative regulation. In fact, the obligation to follow such procedural rites has had a deep impact on their willingness to engage in the rulemaking process, leading to a "dilution of the regulatory process rather than the protection of persons from arbitrary action”.[254] Agencies also release guidance documents, a set of materials to orientate, clarify or interpret rules enacted by the agency, such as staff manuals, interpretative rules, and policy statements. These documents are not subject to notice-and-comment or any other type of rulemaking process, and, because of that, do not have binding effects.

Adjudication refers synthetically to the subsumption of a general rule to a particular case, when administrative action may affect some individual right. Formal adjudication refers to dispute resolution between two or more private parties or the agency and a private party. It occurs when adjudication is "required by statute to be determined on the record after opportunity for an agency hearing”.[255] It resembles a civil trial, with separation between investigation and decision-making. Usually, an Administrative Law Judge – ALJ pronounces the initial decision, which may be reviewed by the agency's head or a commission. On the other hand, the APA does not expressly regulate informal adjudication, although it corresponds to the great part of administrative action. Just as occur in formal adjudication, parties are subject to a decision-making process, which is usually defined in the agency’s own regulation, but differs from the latter, as an on-the-record hearing is not necessarily required. Informal adjudication may include diverse activities, such as planning decisions, advice, guidance, or resource allocation.

When one thinks about regulation, there is a tendency to understand it as a set of activities involving the creation of general and abstract rules that will be applied indistinctly to

[253] CUSTOS, Dominique, The rulemaking power of independent regulatory agencies, **The American Journal of Comparative Law**, v. 54, p. 615–640, 2006. STRAUSS, **Administrative Justice in the United States**.
[254] In 1972, Robert Hamilton had already denounced the lack of disposition of federal agencies to conduct formal rulemaking procedures, observing that “*most of the agencies required to conduct formal hearings in connection with rulemaking, in fact, did not do so in the previous five years*”. HAMILTON, Robert W. Procedures for the adoption of rules of general applicability: the need for procedural innovation in administrative rulemaking. **California Law Review**, v. 60, p. 1276–1338, 1972, p. 1312. The perception that formal rulemaking is notoriously demanding and difficult to manage persists nowadays, cf. STRAUSS, op. cit., p. 306.
[255] APA, §554.

the general public or over a given economic sector. Indeed, the product of rulemaking is more visible to those not familiar with the routine of regulatory activity and even more transparent and accessible when compared with the adjudicatory process, in which is necessary to look at the decision as a whole, its facts, reasoning, and holding to extract a rule.[256] Notwithstanding, both rulemaking and adjudication have been used as regulatory tools to implement public policies. In the FTC, it is no different. However, as will be seen in the next section, the FTC has not relied upon its rulemaking authority to build regulatory policies, but its enforcement powers in special to interpret Section 5 of the FTC Act to combat unfair methods of competition and unfair and deceptive acts or practices.

2.3 THE FEDERAL TRADE COMMISSION IN THE AGE OF DIGITAL PLATFORMS

The Federal Trade Commission is a bipartisan federal agency[257] with a dualistic mission of both protect consumers, by preventing and combating deception and unfair practices, and safeguarding competition, to avoid abusive business practices due to market dominance and foster innovation, a model not adopted in most jurisdictions.[258] As an independent agency, the FTC has more autonomy from the Executive Power than executive agencies, with five commissioners appointed by the U.S. President and approved by the Senate, who serve for a seven-year term.[259] Removal of the commissioners can only occur for cause, which grants the Commission relative protection from political pressures. The Commission is divided into three main bureaus: the Bureau of Competition - BC, in charge of prevention of anti-competitive practices in the marketplace; Bureau of Consumer Protection - BCP, whose mission is to protect consumers against unfair, deceptive, and fraudulent practices; and the Bureau of Economics – BE, which assists the Agency evaluating the economic impact of its regulatory actions. Apart from the bureaus, the FTC also has eight regional offices spread across the United States.

Differently from other administrative agencies, such as the Environmental Protection Agency – EPA or the Food and Drug Administration – FDA, which heavily relies on their rulemaking authority to build a regulatory framework, the FTC has adopted an enforcement-

[256] STRAUSS, op. cit., p. 356-357.
[257] This means that one political party cannot have total control of the head of the agency, which means that the U.S. President will have to consider it when appointing a new commissioner. Thus, in the FTC no more than three commissioners may be members of the same political party of the President.
[258] Most countries have at least two authorities to regulate antitrust and consumer protection matters, some of them with separate jurisdictions (e.g. Argentina, Germany, Israel, India, Japan). For a brief overview of competition and consumer protection authorities across different countries, cf. FTC. **Competition & Consumer Protection Authorities Worldwide**. Washington, D.C. Available at https://www.ftc.gov/policy/international/competition-consumer-protection-authorities-worldwide. Last access on Feb. 21, 2021.
[259] FTC Act, §41.

based approach, modeling its policy essentially through the filing of cases against companies. Due to the broad authority is given especially by Section 5 of the FTC Act,[260] a strong and open-ended mandate, which allows the Agency to fight against 'unfair methods of competition' as well as 'unfair and deceptive practices', the Commission has expanded its authority and updated its understandings accordingly to technological advances. As will be seen in the next subsections, although the FTC has the authority to enforce other statutes apart from the FTC Act, most of FTC action relates to violations of Section 5. Indeed, FTC orders based on Section 5 of the FTC Act have been an important mechanism to regulate information privacy matters in the United States at the federal level, since there is no general statute covering this field of law.

Apart from its enforcement authority, the Commission also develops an extensive non-litigation program. To provide clarity to regulated actors about the Commission's interpretations and rules, the Agency also undertakes educational campaigns and holds multistakeholder workshops to debate public policies approaches and hear private sector concerns.[261] The Agency also regularly issues guidance documents, such as reports, advisory opinions, and studies. As seen in the last section, guidance documents are not subject to procedural constraints of rulemaking and, because of that, they do not necessarily bound the Agency's decisions. Yet, companies tend to take into account the orientations provided by these documents, as they signal the positions adopted by the Commission. In this context, it is relevant to analyze in the next subsections whether and how the FTC has developed a regulatory policy for digital platforms.

In recent years, the FTC has become a key actor in the regulation of platforms debate. The dual mandate to protect consumers and competition, in the context of digital platform markets, gives regulatory authorities a privileged view of complex and enchained markets, as digital markets are, and represents an opportunity to develop more consistent and coordinated regulatory policies to target effectively those businesses. As seen in the previous chapter, platforms, the paradigmatic business in the informational capitalism era, exert power over different strands of society given their gatekeeping role. Their immense control over information flows, shaping the social debate, consumer habits and relationships relies on surveillance apparatus built to extract quantity and diversity of data. Use of the Internet for a

[260] FTC Act, §45 (a) (1) (2). The FTC was originally created with the mission of ensuring fair competition in commerce. With the Wheeler-Lea Amendment of 1938 to section 5 to the FTCA, Congress extended Commission's power to prevent deceptive and unfair acts or practices.
[261] HOOFNAGLE, op. cit.

great part of users consists in navigating through the intermediation of these few firms, which gives them a great persuasion power – from the contacts to follow in social networks to the restaurant to have dinner that appears in the search results. Surveillance capacity alone, though, is not enough to explain the dominance of those companies. In a fast-changing and highly innovative market, is necessary to keep a step ahead of opponent firms, through either an aggressive research and development strategy or a good eye to identify ascending firms – potential rivals - and snap them before they are too big to compete. The next subsections will provide a deeper explanation about these two competences undertaken by the FTC, focusing on the regulation of digital markets.

2.3.1 The FTC as Information Privacy Regulatory Authority

Some privacy scholars consider rules about the use and collection of personal data in the United States weak and limited.[262] A recurrent complaint lies in the fact that there is no unitary online privacy statute along with the lines of the E.U.'s GDPR in the country. The different regulatory approach between EU and US regarding the right to privacy escalated in 2020, when the European Court of Justice (ECJ), in *Schrems II* case, considered the US-EU data protection agreement (Privacy Shield) invalid, as it could not afford an adequate level of privacy to European citizens' data when transferred to the United States.[263] However, information privacy is indeed seen as an issue to be regulated, and there have been some developments in recent years, especially through the FTC action.

[262] RICHARDS, Neil M. The Dangers of Surveillance. **Harvard Law Review**, v. 126, p. 1934-1965**,** 2013, p. 1942; BROOKMAN, Justin. Protecting Privacy in an Era of Weakening Regulation, **Harvard Law Review**, v. 9, 355-374, 2015, p. 356. ("Despite the persistent consumer concern about commercial data collection, the legal framework to protect privacy and personal data in the United States is quite weak, both absolutely and especially when compared with the rest of the world").

[263] For a brief analysis about Schrems II, see BIGNAMI, Francesca. Scherms II: the right to privacy and the new illiberalism. Verfassungsblog, Jul 29, 2020. Available at https://verfassungsblog.de/schrems-ii-the-right-to-privacy-and-the-new-illiberalism/. Last access Nov. 20, 2020.

The United States information privacy law derives from the Constitution,[264] common law,[265] state law[266] and limited-scope federal statutes that target either a specific type of information[267] or certain groups of people.[268] As result, while some economic sectors are subject to detailed statutory obligations (e.g. credit report agencies to FCRA), other pivotal sectors (e.g. the technology industry) seem to remain lightly regulated (or not regulated at all) in matters of information privacy.[269] However, the fragmentary character of the privacy framework does not mean businesses that do not fall on the scope of any of those statutes – the majority part of business indeed – are not free from information privacy regulation, as they are subjected to FTC's authority.

The FTC, as an independent agency, was originally created to promote competition. With the Wheeler-Lea Amendments in 1938, Commission received the mission to take action against practices that would violate consumer's rights. However, it was not until the late 1990s that the Agency started to enter the information privacy realm. With the popularization of Internet access and the discovery of the potential of users' data collection through cookies and other technologies, allied with the pressure to meet adequate levels of protection prescribed in the EU Data Protection Directive 95/46/EC, the Agency slowly started to enforce online privacy matters. Through the last decades, the FTC has managed to expand its jurisdiction over online privacy in a way that many consider it functions as a *de facto* privacy authority.[270]

---

[264] The United States Constitution does expressly mention a right to privacy. However, this right can be extracted from the First Amendment's right to assemble and right to speak anonymously, from the Third Amendment, which protects the right to privacy at home ("No Soldier shall in time of peace be quartered in any house…") and from the Fourth Amendment that provides the right of people "to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures".

[265] The privacy right was firstly identified in the famous Warren and Brandeis article *The Right to Privacy*, in which they advocate for the recognition of privacy as a new category of right, a 'right to be left alone'. Decades later, William Prosser identified four causes of action for invasion of privacy torts law (intrusion upon seclusion, public disclosure of private facts, false light, and appropriation). Privacy is also protected by contract law, through specific contractual protection related to disclosure of personal information.

[266] Many State Constitutions have a privacy clause. As well, states have also passed statutory laws protecting the right to privacy in different contexts (medical data, financial privacy, data breach, and others).

267 See, for instance, the Fair Credit Reporting Act of 1970, USC, Title 15 §§ 1681-1681x (provides citizens with rights regarding the use and disclosure of their personal information by credit reporting agencies); the Health Insurance Portability and Accountability Act of 1996 (gives the Department of Health and Human Services – HHS the authority to promulgate regulations governing the privacy of medical records); Family Educational Rights and Privacy Act of 1974 (protects privacy of student education records).

268 See Children's Online Privacy Protection Act of 1998, USC, Title 15 §§ 6501-6506 (restricts the use of information gathered from children under 13 by Internet websites); Driver's Privacy Protection Act of 1994 (protects privacy of personal information assembled in the State Department of Motor Vehicles).

269 DAVIS, Ian M. Resurrecting Magnuson-Moss Rulemaking: the FTC at a data security crossroads. **Emory Law Journal**, v. 69, n. 4, 2020 (considering that there are some advantages in sectorial-focused privacy statutes, as it permits it allows the construction of a more detailed regulation that is closer to the reality of the economic sector).

[270] HETCHER, Steven. The De Facto Federal Privacy Commission, **Journal of Computer & Information Law**. v. 19, n. 1, 2000. SOLOVE; HARTZOG, op. cit., 2014; HOOFNAGLE, op. cit.

To pursue its goals of protecting consumers' privacy, the Commission heavily relies on case-by-case enforcement under the FTC Act. Besides, over years, Congress has appointed the Commission as responsible for the enforcement of a series of privacy-related statutes, such as the Children's Online Privacy Protection Act,[271] the Fair Credit Reporting Act[272], the Gramm-Leach-Biley Act,[273] Telemarketing and Consumer Fraud and Abuse Prevention Act[274] and the Identity Theft Assumption and Deterrence Act.[275] There are many divisions in the BCP responsible for the regulation of privacy matters,[276] but the Division of Privacy and Identity Protection – DPIP, in particular, has been responsible for topics related to consumer privacy, credit reporting, identity theft, and information security.[277] The DPIP is in charge of almost all privacy policies undertaken by the Commission, not only through the enforcement of privacy and security cases but also by issuing reports and conducting workshops related to information privacy.[278]

One might ask why the Commission, as an independent agency with *quasi*-legislative and *quasi*-judicial powers, and considering the inexistence of comprehensive federal privacy statute, relies on a case-by-case enforcement approach rather than engaging in rulemaking to fill legal gaps in matters of information privacy. Although Congress did not grant the FTC rulemaking authority over privacy matters specifically, the Commission has it to promulgate regulations over "*acts or practices which are unfair or deceptive acts or practices in or affecting commerce*", which derives from the 1975 Magnuson-Moss Warranty Act (Magnuson-Moss Rules).[279] Magnuson-Moss Rules provide the only rulemaking authority for the FTC to engage

[271] UNITED STATES. USC. Title 15 §§ 6501-6506. Available at https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.

[272] UNITED STATES. USC. Title 15 U.S.C. §§ 1681-1681x. Available at https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act.

[273] UNITED STATES. USC. Title 15 U.S.C § 6801-6827. Available at https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act.

[274] UNITED STATES. USC. Title 15 U.S.C. § 6101-6108. Available at https://www.ftc.gov/enforcement/statutes/telemarketing-consumer-fraud-abuse-prevention-act.

[275] UNITED STATES. USC. Title 18 U.S.C. § 1028. Available at https://www.ftc.gov/enforcement/statutes/identity-theft-assumption-deterrence-act-1998.

[276] The BCP has eight divisions: the division of Privacy and Identity Protection, Advertising Practices, Consumer & Business Education, Enforcement, Marketing Practices, Consumer Response and Operations, Litigation Technology and Analysis, and Financial Practices. FEDERAL TRADE COMMISSION, **FTC's Bureau of Consumer Protection**. Available at https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection. Last visited Mar. 14, 2021.

[277] FEDERAL TRADE COMMISSION. **FTC's Division of Privacy and Identity Protection**, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-privacy-and-identity. Last visited Mar. 14, 2021.

[278] Cf. e.g. FEDERAL TRADE COMMISSION, op. cit., 2016.

[279] UNITED STATES. USC. Title 15 §§2301-2312, Magnuson-Moss Warranty—Federal Trade Commission Improvement Act. Available at https://www.ftc.gov/enforcement/statutes/magnuson-moss-warranty-federal-trade-commission-improvements-act. According to the FTC Act, "Except as provided in subsection (h) of this

in rulemaking regarding unfair and deceptive acts or practices. It differs from the notice-and-comment procedure depicted in the APA, as it demands additional acts, such as publication of an advanced notice of proposed rulemaking to be submitted to the several congressional committees and holding of an informal hearing,[280] but does not require the following of all the steps presented on formal rulemaking, being a species of hybrid rulemaking.

However, due to the necessity to perform a series of acts and formalities, the Commission has considered the Magnuson-Moss rulemaking procedure too lengthy and has largely ignored this rule.[281] Indeed, to accomplish with Magnuson-Moss Rules, the FTC staff must undertake a series of procedures too burdensome. When compared the average time spent in FTC rulemaking before and after the enactment of the Magnuson-Moss Rules, it is undeniable that the Commission took considerably more time to issue regulations: pre-Magnuson-Moss Act rules were enacted on 2.94 years approximately, whereas after the adoption of the Magnuson-Moss Act the average time practically doubled, taking 5.57 years for enactment.[282] Enthusiasts of the case-by-case model consider that the Magnuson-Moss Act procedures are so burdensome and time-consuming that would not be able to follow the rapid pace of the technology industry.[283] Time and efforts spent in the enactment of a broad regulation, and the subsequent procedural difficulties to update them, would lead the Agency always one step behind. The question that remains is that whether *ex-post* regulation through enforcement has been able to accompany the dynamic data-centered industry.

Thus, it is not exaggerated to state that Section 5(b) of the FTCA, which protects consumers "*unfair or deceptive acts or practices affecting commerce*", has been the driving force of U.S. information privacy law. Section 5 of the FTCA is a comprehensive mechanism

---

section, the Commission may prescribe rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce (within the meaning of section 45(a)(1) of this title), except that the Commission shall not develop or promulgate any trading rule or regulation with regard to the regulation of the development and utilization of the standards and certification activities according to this section. Rules under this subparagraph may include requirements prescribed for the purpose of preventing such acts or practices". FTC Act, §57a (a)(B).

[280] FTC Act §57a (b)(2)(A)(B); FTC Act §57a (c).

[281] DAVIS. op. cit., p. 786 ("Despite its congressional grant of rulemaking authority, the FTC has declined to promulgate a regulatory rule identifying the boundaries of unlawful data security"); HOOFNAGLE. op. cit., 100 ("The rule-making structure created by Congress in the Magnuson-Moss act is considered a failure by the Commission and is unlikely to be used for privacy matters").

[282] LUBBERS, Jeffrey S, It's Time to remove the "mossified " procedures for FTC rulemaking, **The George Washington Law Review**, v. 83, n. 6, p. 1979–1998, 2015.

[283] HOOFNAGLE, op. cit., p. 55 ("Burdensome procedures are one of the main reasons why the FTC has not sought to promulgate rules for privacy - the thought that by the time the procedures are satisfied, any privacy rule would be out of date"); SOLOVE; HARTZOG, op. cit., p. 620 ("Although the FTC has specific rulemaking authority under COPPA and GLBA, for Section 5 enforcement—one of the largest areas of its jurisprudence—the FTC has only Magnuson-Moss rulemaking authority,175 which is so procedurally burdensome that it is largely ineffective").

of regulatory action in the matter of privacy and allowed a significant expansion of the Commission's authority, given its open language and encompassing reach of FTC authority over different economic sectors. Congress, in its turn, deliberately chose not to define what would constitute a deceptive or unfair practice and delegated this task to the Commission, because technologies and businesses practices were in constant evolution. The concept of deception and unfairness should be a dynamic one, which would permit the FTC to adapt quickly to new social and economic contexts. In turn, the Judiciary branch has upheld broad interpretations of the FTC jurisdiction under Section 5 of the FTCA.[284] In the matter of privacy specifically, the U.S. Court of Appeals for the Third Circuit affirmed in *FTC* v. *Wyndham Worldwide Corp.* that the Commission had the authority to regulate cybersecurity under section 5 of the FTC Act. Commenting on the *Wyndham* decision FTC's Chairwoman Edith Ramirez wrote that "Third Circuit Court of Appeals decision reaffirms the FTC's authority to hold companies accountable for failing to safeguard consumer data".[285] Such legal constructions allowed the Agency to grow confident about the scope of its activities and to ascend as the primary privacy regulator in the United States.

Through the development of theories of deception and unfairness practices depicted in section 5 of the FTC Act and sectorial statutes, the FTC has developed a privacy regulation framework through a case-by-case approach that resembles common law and grows thicker as it develops.[286] As observed by Solove and Hartzog, under section 5 of the FTCA, the FTC

[284] UNITED STATES. United States Court of Appeals, Third Circuit. FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (2015). Aug. 24, 2015. Available at https://caselaw.findlaw.com/us-3rd-circuit/1711436.html ("Congress explicitly considered, and rejected, the notion that it reduce the ambiguity of the phrase 'unfair methods of competition'…by enumerating the particular practices to which it was intended to apply… the takeaway is that Congress designed the term as a flexible concept with evolving content"); UNITED STATES. Supreme Court. FTC v. Colgate-Palmolive Co., 380 US 374, 385 (1965). April 5, 1965. Available at https://supreme.justia.com/cases/federal/us/380/374/. ("Moreover, as an administrative agency which deals continually with cases in the area, the Commission is often in a better position than are courts to determine when a practice is 'deceptive' within the meaning of the Act. This Court has frequently stated that the Commission's judgment is to be given great weight by reviewing courts. This admonition is especially true with respect to allegedly deceptive advertising since the finding of a Section 5 violation in this field rests so heavily on inference and pragmatic judgment"); and UNITED STATES. United States Court of Appeals, Tenth Circuit. FTC v. Accusearch Inc., 570 F. 3d 1187 (2009). Jun. 29, 2009. Available at https://bit.ly/3iCnfjw ("Its premise appears to be that a practice cannot be an unfair one unless it violates some law independent of the FTCA. But the FTCA imposes no such constraint. *See* 15 U.S.C. § 45(n) (setting out elements of an unfair practice). On the contrary, the FTCA enables the FTC to take action against unfair practices that have not yet been contemplated by more specific laws").

[285] FEDERAL TRADE COMMISSION, **Statement from FTC Chairwoman Edith Ramirez on Appellate Ruling in the Wyndham Hotels and Resorts Matter**. [Washington], Aug. 24, 2015. Available at https://www.ftc.gov/news-events/press-releases/2015/08/statement-ftc-chairwoman-edith-ramirez-appellate-ruling-wyndham.

[286] SOLOVE; HARTZOG, op. cit., 2014. However, it does not mean that the FTC Act's interpretation relies on common law. On the contrary, the FTC Act rejects in many aspects some common law approaches to consumer protection, such as no need for the Commission to show intent to deceive or proof of harm. HOOFNAGLE, Chris

developed a rich body of privacy settlements, called 'consent orders', which, despite their lack of precedential force,[287] functions as the primary source of privacy regulation at a federal level.[288] *Wyndham* case is particularly important to corroborate this approach, as the Third Circuit withheld Wyndham's argument that FTC must have set data-security standards in advance. In fact, the Third Circuit considered that, under the Due Process Clause of the U.S. Constitution, fair notice does not require a narrowly tailored definition of unlawfulness.[289] Fair notice is accomplished if "*the company can reasonably foresee that a court could construe its conduct as falling within the meaning of a statute*".[290] This decision was particularly important to rule out any understanding that the FTC could only regulate data security through rulemaking.

Therefore, if the FTC has reason to believe that the targeted company violated section 5 of the FTC Act, the Commission, after a period of investigation, can use its enforcement powers to issue a complaint through administrative or judicial litigation. The defendant company can either settle with the Commission, through a consent decree, or contest the complaint, either administratively or before a federal district court. Firms tend to prefer to settle an agreement because it does not imply recognition of the unlawful practices and the terms of the settlement tend to be smoother than if they litigate and do not succeed. Consent decrees must be approved by the majority of the Commissioners and function as a contract between the company and the FTC, which imposes a bundle of restraints and obligations to be followed by the defendant company, which shall be subjected to the terms of the consent order for a long period, usually 20 (twenty) years. The construction of this common law of privacy does not limit to the issuance of consent decrees that should be followed by the regulated industries, though. When a case is submitted to administrative jurisdiction, the Commission releases the complaint and submit the consent decree to public comment for 30 days. During the comment period, industry, academia, and civil society may submit written contributions about the clauses of the order. Although restricted and not binding, it represents an effort to increase social participation in the agency decision-making process and receipt of feedback. After this period, the FTC approves the final terms of settlement and enters the consent order, the final settlement which is mandatory to the firm.

Jay, FTC Regulation of Cybersecurity and Surveillance, *in*: GRAY, David; HENDERSON, Stephen E. (Orgs.), **The Cambridge Handbook of Surveillance Law**, New York: Cambridge University Press, 2017, p. 708–726, p. 710-711.

[287] SOLOVE; HARTZOG, op. cit., p. 619.

[288] Ibid., p. 588 and 600.

[289] FTC v. Wyndham Worldwide Corp. p. 249.

[290] Ibid., p. 256.

In case of contesting the complaint administratively, the case is decided by an FTC administrative law judge (ALJ), and both the parties can appeal from the ALJ decision to the Commissioners, which will issue the final decision. If the respondent company does not agree with the FTC's verdict, it may pursue judicial review through the filing of an appeal before a court of appeal. This process, though, is extremely costly, so businesses usually have incentives to settle with the Commission at the first opportunity. Reaching an agreement with the Commission is also advantageous because the FTC cannot apply direct civil penalties when a company violates section 5 of the FTC Act. Penalties can only be imposed in case of a breach of the consent order. The FTC may issue civil penalties of not more than $10,000 per violation.[291] The observation of such settlements and consent orders reveals to be of extreme importance for those lawyering in this field as they are explicit what conducts the agency considers as a violation of the law and the best practices to be followed.[292]

The FTC has an extremely broad interpretation of deception and unfairness, but it does not mean that the Commission's action has no standards. Analysis of unfairness and deception practices must follow the standards depicted in the Policy Statement on Deception (1984) and the Policy Statement on Unfairness (1980). The codification of these standards was important to respond to multiple critics about the inconstancy and lack of criteria of the Commission while engaging in enforcement actions against companies.[293] The FTC Policy Statement on Deception aimed to bring some light to the contours of such practices. According to the Statement, three elements sustain all deception cases: (1) an omission, a distortion, a misrepresentation that is likely to lead consumers to error; (2) it concerns a circumstance that had she had more information, would have acted differently; and (3) the omission or practice must be material.[294] When analyzing the first element, the FTC does not have to prove that the consumer was actually misled, but only that the act had the potential to mislead.[295] A misrepresentation consists of an express or implied statement opposed to a given fact, whereas a misleading omission refers to the lack of disclosure of meaningful information.[296] The second element should be interpreted from the perspective of a 'reasonable consumer', which means that not all misconceptions will necessarily lead to an unlawful action under Section 5. Notwithstanding, when the FTC assesses

[291] FTC Act, §45 (m)(1)(A).
[292] SOLOVE; HARTZOG, op. cit., 2014, p. 607.
[293] HANS, G. S., Privacy Policies, Terms of Service and FTC Enforcement: broadening unfairness regulation for a new era, **Michigan Telecommunications & Technology Law Review**, v. 19, n. 1, p. 163–197, 2012, p. 171.
[294] FEDERAL TRADE COMMISSION. **FTC Policy Statement on Deception.** Washington, Oct. 14, 1983. Available at https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.
[295] Id.
[296] HOOFNAGLE, op. cit., 2016, p. 123.

a possible deceptive practice, it takes into account the whole consumer experience and particular circumstances of the audience.[297] The last element refers to the materiality of the act or practice, meaning whether the information is likely to affect consumers' choices.[298] There is no need to prove consumer injury in deception cases, as this analysis is embedded in the materiality of the misleading information, because the practice that affected the consumer's choice may cause harm.[299] Nor is necessary to prove the defendant's intent to mislead or deceive. In the early years enforcing information privacy matters, the FTC adopted a cautious pace, beginning with addressing deception practices.

The enforcement of deceptive practices is rooted in the notice-and-choice model, which had prevailed in the first cases regarding information privacy in consonance with the self-regulatory approach to Internet matters dominant at the beginning of this century, and helped the Commission to consolidate its authority in this realm. The reliance on self-regulation as the "best and most efficient way" to regulate privacy matters on the Internet was made clear in Commissioners Orson Swindle and Thomas B. Leary's joint dissenting statement in *Federal Trade Commission v. ReverseAuction.com, Inc* case.[300] Although the Commission voted unanimously for the existence of deceptive practices in the case, Commissioners Swindle and Leary made clear in their statement their disagreement in supporting unfairness theory in the first count of the case, defending that theory of deception would fit better in the self-regulatory environment and the adequate level of government intervention on online privacy protection.[301] Although defeated by the majority, this case shows, at that time, the understanding that self-regulation would better serve online privacy.

Deception analysis departs from an idea of privacy as control over personal information, individuals should be free to choose to disclose their personal information or not, but they should be fully informed about what information was being disclosed and for which purposes. In early cases such as *In the Matter of GeoCities* and *In the Matter of Eli Lilly*, the FTC focused on privacy representations made by companies through the policies depicted in their websites

[297] Id.
[298] Federal Trade Commission, op. cit., 1983.
[299] SERWIN, op. cit.
[300] FEDERAL TRADE COMMISSION. **Federal Trade Commission v. ReverseAuction.com**, Inc. Civil Action No. 000032, D.D.C. Jan 6. 2000. (Statement of Comm'rs Orson Swindle and Thomas B. Leary). Available at https://www.ftc.gov/sites/default/files/documents/cases/2000/01/www.ftc_.gov-reversesl.htm.
[301] FEDERAL TRADE COMMISSION. Federal Trade Commission v. ReverseAuction.com. Years before, Commissioner Swindle had already expressed in his vote in Geocities his reservation in applying section 5 remedy to other commercial internet sites.

regarding personal data sharing with third parties.[302] Similarly, in *In the Matter of Google, Inc.*, the FTC considered as deceptive Google's inadequate notice that some information provided in Google Buzz would be shared as public by default.[303] Besides, the Commission considered Google Buzz's privacy settings were confusing and difficult to find and found unlawful Google's practice of sharing Gmail users' personal information to Google Buzz, automatically creating a profile to them, probably to foster the use of the company's new social network, without any prior consent.[304]

However, a deception analysis solely based on promises made through privacy policies would be too restrictive and would constitute an incentive for companies to implement vague commitments. For the notice and choice approach to be truly effective, companies must give conditions to consumers to make more informed and meaningful choices.[305] It includes clear and simple explanations about data practices, including what data they collect and with whom they share.[306] Thus, the FTC has expanded the notion of deceptive practices in order to encompass any representation, made through any means, by the companies regarding information privacy, as well as omissions about the collection and use of data. When analyzing a potential deceptive practice or action, the FTC understands that companies must disclose prominently information collection or uses that violate consumer expectations.[307] Such a comprehensive approach turned to be efficient for the Commission to act against a vast array of surveillance practices. In *In the Matter of Sears Holding Management Corporation*, Sears, a popular department store, paid consumers ten dollars for them to install an application in their computers to track their browsing activities.[308] However, the tracked information included not

[302] FEDERAL TRADE COMMISSION. **In the Matter of GeoCities**. Docket No. C-3850, File No. 9823015, Feb. 12, 1999. (Complaint) Available at https://www.ftc.gov/sites/default/files/documents/cases/1999/02/9823015cmp.htm; FEDERAL TRADE COMMISSION. **In the Matter of Eli Lilly and Co.**, Docket No.C-4047, File No. 0123214, May 10, 2002. Available at https://www.ftc.gov/sites/default/files/documents/cases/2002/05/elililllycmp.htm.

[303] FEDERAL TRADE COMMISSION. **In the Matter of Google, Inc.** Docket No. C-4336, File No. 1023136, October 23, 2011. (complaint) Available at https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzcmpt.pdf.

[304] Id.

[305] FEDERAL TRADE COMMISSION. **Protecting consumer privacy in an era of rapid change:** recommendations for business and policymakers, Washington: [s.n.], Mar. 2012 Available at https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

[306] Ibid.

[307] HOOFNAGLE, Chris Jay, FTC Regulation of Cybersecurity and Surveillance, *in*: GRAY, David; HENDERSON, Stephen E. (Orgs.), **The Cambridge Handbook of Surveillance Law**, New York: Cambridge University Press, 2017, p. 708–726, p. 712.

[308] FEDERAL TRADE COMMISSION. **In the Matter of Sears Holding Management Corp.** Docket No. C-4264, File No. 0823099, June 4, 2009. (complaint) Available at https://www.ftc.gov/sites/default/files/documents/cases/2009/09/090604searscmpt.pdf.

only information about websites consumers visited and links that they clicked, but also such as online banking statements, video rental transactions, online drug prescription records, and select header fields that could show the sender, recipient, subject, and size of web-based email messages. The Commission considered that, despite the existence of an agreement between Sears and consumers, the company did not prominently disclose the extension of web tracking practices.

As data collection becomes ubiquitous, with technology companies entering offline spaces to collect data, either through tracking mechanisms or the popularization of IoT devices, the FTC has advocated for consumer awareness and the possibility to opt out. In *In the Matter of Nomi Technologies, Inc.*, for instance, the Commission filed a complaint against Nomi, a company that provides a tracking technology to retailers follow consumers' movement and collect their mobile phone information through their stores.[309] Nomi provided analytics reports about aggregate consumer traffic including the percentage of consumers that passed by the store compared with those who entered; average time of consumers' visits; types of mobile devices and so forth. The company's privacy policy allowed consumers to opt out through its website but did not provide a list of retailers using the service or any information about the usage of the tracking technology while consumers were at the stores.[310] Similarly, the FTC found deceptive Vizio's privacy policies regarding its smart TVs. Vizio remotely installed in smart TVs previously sold a software that collected information about the television, programs, and advertisements watched, IP address, WiFi signal strength, and other data. This data later was share with third parties.[311] However, as consumers had not received any notice about the software installation or the data sharing with other parties, the Commission considered that Vizio's conduct constituted a deceptive practice.[312]

The theory of deception also encompasses misrepresentations regarding security measures undertaken by companies. In *In the Matter of Snapchat*, the FTC challenged the application's statement that photos and videos sent through its messaging service would

[309] FEDERAL TRADE COMMISSION. **In the Matter of Nomi Technologies, Inc.** Docket No. C-4538, File No. 1323251, Sep. 3, 2015. (Complaint). Available at https://www.ftc.gov/system/files/documents/cases/150902nomitechcmpt.pdf.
[310] Ibid.
[311] FEDERAL TRADE COMMISSION. **FTC v. Vizio, Inc. and Vizio Inscape Services, LLC**. Case 2:17-cv-00758, US District Court District of New Jersey, Feb. 3, 2017. (Complaint) Available at https://www.ftc.gov/enforcement/cases-proceedings/162-3024/vizio-inc-vizio-inscape-services-llc.
[312] Ibid.

disappear within seconds, despite the existence of mechanisms to recover the media.[313] The FTC also found deceptive Uber's promises to provide reasonable security standards regarding internal access and storage of personal data, which led the ride-sharing application to face two data breaches.[314]

On the other hand, declaring a practice is unfair, rather than deceptive, tends to be more sensitive.[315] While deceptive practices involve the statement of imprecise or false information or even an omission that may mislead the user, unfairness involves a practice that causes substantial consumer harm. As result, the usual remedy to those practices is to give better notice or ask users for consent, whereas a practice labeled as 'unfair' may not subsist and the defendant company should ban it. Therefore, the FTC has been historically more cautious in the appliance of the unfairness theory in information privacy and security matters, although it has expanded its use in more recent cases.[316] The three factors to define whether an act or practice is unfair were first outlined in *FTC v. Sperry & Hutchinson Co.* by the U.S. Supreme Court.[317] To be unfair, the act must configure a (1) consumer injury (2) that violates an established public policy (3) through a practice unethical or unscrupulous.[318] Nowadays, the three consumer injury requirements are codified in Section 5(n) of the FTC Act stating that when "*determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination*."[319] The violation of an 'established' public policy, that is, the one settled in a statute, judicial decisions, industry practice, or otherwise.[320] On the other hand, the Commission has not taken into account the unethical conduct factor separately for considering it 'largely duplicative', as both consumer injury and established public policies requirements would encompass it.[321]

---

[313] FEDERAL TRADE COMMISSION. **In the matter of Snapchat.** Docket No. C-4501, File No. 1323078, Dec 14, 2014. (complaint) Available at https://www.ftc.gov/enforcement/cases-proceedings/132-3078/snapchat-inc-matter.
[314] FEDERAL TRADE COMMISSION. **In the matter of Uber Technologies, Inc.** Docket No. C-4662, File No. 1523054, Oct. 25, 2018. (Complaint) Available at https://www.ftc.gov/enforcement/cases-proceedings/152-3054/uber-technologies-inc.
[315] HOOFNAGLE, op. cit, 2016.
[316] SOLOVE; HARTZOG, op. cit., 2014, p. 638.
[317] UNITED STATES. Supreme Court. FTC v. Sperry & Hutchinson Co. 405 U.S. 233 (1972). Available at https://supreme.justia.com/cases/federal/us/405/233/.
[318]FEDERAL TRADE COMMISSION. **FTC Policy Statement on Unfairness.** Washington, Dec. 17, 1980. Available at https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.
[319] FTC Act, U.S.C. §45 (n).
[320] FEDERAL TRADE COMMISSION, op. cit., 1980.
[321] HOOFNAGLE, op. cit., p. 133.

In 1980, the Commission issued a Policy Statement on Unfairness to outline the criteria to be followed when staff investigates a potential unfair act or practice. According to the Statement, to assess consumer injury, the first requirement, the defendant must pass a three-prong test: (1) the practice has to cause substantial injury, (2) which is not reasonably avoidable by the consumer herself, and (3) cannot be outweighed by countervailing benefits to competition or consumer as a consequence of the practice. The Commission's analysis historically has heavily weighted the existence of substantial consumer injury, so it must convincingly demonstrate it to find a practice unfair.

The analysis of unfairness is identified with the harms-based approach, focused on addressing monetary, health, and physical injuries. Thus, consumer injury does not encompass emotional distress and "other more subjective types of harm".[322] However, the FTC has expanded the unfairness doctrine in privacy cases and addressed a wider range of injuries. For instance, in *FTC v. Accusearch*, the Commission considered that defendant's conduct of make available names and telephone records online without consumers' consent led them to incur emotional harm, due to the risk of being stalked or harassed, and caused substantial harm, so the conduct was unfair under Section 5.[323] The second injury factor, that is, the conduct not reasonably avoided by the consumer, the Commission would act when consumers are prevented from making their own decision.[324] The third injury factor involves a cost-benefit analysis between the assessed burdens placed upon consumers and gains perceived with the act or practice.[325]

The FTC has considered unfair acts and practices that undermine consumer confidence in commercial relations. Among those practices, the Commission condemned retroactive changes in privacy policies, that is, modifications in a company's policies without prior notice or consent of users. The Commission considered particularly unlawful configuration changes that set as default privacy choices not expressly consented by consumers from which they have to opt-out.[326] The FTC also considers unfair acts or practices those through which companies collect or use data fraudulently. For instance, in *In the Matter of ReverseAuction*, the website ReverseAuction.com unduly collected E-Bay's users' data to send a series of unsolicited e-mails

[322] FEDERAL TRADE COMMISSION, op. cit., 1980.
[323] UNITED STATES. **FTC v. Accusearch, Inc**.
[324] FEDERAL TRADE COMMISSION, op. cit., 1980.
[325] Id.
[326] FEDERAL TRADE COMMISSION. **In the Matter of Gateway Learning Corp.**, FTC File No. 042 3047, Sep. 17, 2004. (Complaint) Available at https://www.ftc.gov/enforcement/cases-proceedings/042-3047/gateway-learning-corp-matter; FEDERAL TRADE COMMISSION. **In the Matter of Facebook, Inc.**, FTC File No. 092 3184, Jul. 27, 2012. Available at https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc.

leading many of them to believe that their E-Bay account was about to expire. Similarly, in *FTC v. Accusearch,* the defendant company collected consumers' telephone records through fraudulent statements and other misrepresentation to induce carrier's employees and agents to disclose confidential information.[327] In matters of data collection particularly, the Commission deemed as unfair the collection of sensitive data without consumer proper notice.[328] Sensitive data includes medical records, precise geolocation data, financial data, social security numbers, and children's data.[329]

When compared to deception, unfairness theory focuses on harm rather than on representations of firms regarding privacy commitments. As result, it can achieve not only the individuals who have a relationship with the defendant company but also those who, by any chance were injured and had their privacy rights violated. In this sense, the FTC charged with unfairness a shopping cart company that provided services to online merchants for sharing personal data of the merchants' customers with third parties, regardless of the merchants' privacy policies and commitments and without their consent.[330] Therefore, the unfairness doctrine is especially relevant to fill the gap left by deception theory upon which notice and choice model relies on and target industries not covered by sectorial statutes, which limits collection and processing of financial data.

If in the early 2000s, the FTC primarily relied on self-regulation and played a role as enforcer of private promises, it also allowed a slow and cautious penetration of the Commission in the privacy realm in a time when there was a strong rejection of governmental interference on online business. Both notice and choice and harm-based models have suffered critics, the first for result in lengthy and complex privacy policies that no one actually reads and the latter for not reflect the harms derived from privacy violations.[331] However, with time, the flexibility of deception and unfairness standards allowed the FTC to develop a body of privacy obligations and gradually expand its authority in this realm toward a more comprehensive privacy

[327] UNITED STATES, **FTC v. Accusearch, Inc**.
[328] FEDERAL TRADE COMMISSION. **Vizio, Inc. and Vizio Inscape Services, LLC**. In a separate statement, Commissioner Maureen K. Ohlhausen questioned the policy reasons to classify granular television viewing information as sensitive data and claimed the Commission to examine more rigorously the concept of substantial injury in the context of consumer data. (Concurring Statement of Acting Chairman Maureen K. Ohlhausen In the Matter of Vizio, Inc.). Available at https://www.ftc.gov/public-statements/2017/02/concurring-statement-acting-chairman-maureen-k-ohlhausen-matter-vizio-inc.
[329] FEDERAL TRADE COMMISSION, **Protecting consumer privacy in an era of rapid change**, p. 59.
[330] FEDERAL TRADE COMMISSION. **In the Matter of Vision I Properties, LLC et al.** Docket No. C-4135, File No. 0423068, Apr. 26, 2005. Available at https://www.ftc.gov/enforcement/cases-proceedings/042-3068/vision-i-properties-llc-et-al-matter.
[331] HOOFNAGLE, op. cit., 2016; NEHF, James P. The FTC's proposed framework for privacy protection online : a move toward substantive controls or just more notice and choice ? **William Mitchell Law Review**, v. 37, n. 4, p. 1727–1744, 2011.

framework. In this sense, the shift from privacy promises to privacy expectations was a pivotal one. Instead of analyzing what companies have promised through their privacy policies, the Commission has focused on consumers' expectations of privacy, so it must take into account shreds of evidence, such as architectural choices, context, functionalities, general statements, and cognitive limitations.[332] Despite the advances undertaken by the Commission, as will be seen in the next chapter, enforcement action to regulate effectively platforms and other information age businesses have limitations and still need improvements.

2.3.2 The FTC as competition authority in digital platforms markets

Along with the Department of Justice Antitrust Division, the Federal Trade Commission's Bureau of Competition has been responsible for the enforcement of antitrust law and protection of competition for benefit of consumers. Although their authority over anticompetitive practices may overlap in some circumstances, both agencies have worked in a coordinated fashion to avoid duplicated efforts.[333] The FTC has exclusive authority to enforce prohibition against "unfair methods of competition" in the FTC Act,[334] as well as, concurrently with the DOJ, anticompetitive conducts depicted in the Clayton Act,[335] a statute crafted to deal with practices that would lead to the constitution of a monopoly, such as mergers and price-fixing agreements. The DOJ has authority to enforce the Sherman Act,[336] which proscribes every agreement in restraint of trade (section 1) and unilateral conducts that monopolize or attempts to monopolize the relevant market (section 2). Most of the penalties for violating of Sherman Act are civilian, but the statute also depicts criminal conducts, such as formation of cartels. Currently, the FTC competition mission is also responsible for mergers, in special the premerger notification program introduced by the Hart-Scott-Rodino Antitrust Improvements

[332] SOLOVE; HARTZOG, op. cit. 2014, p. 667.
[333] Each agency has been devoting resources and acquiring expertise in certain markets. The FTC, for instance, has orientated its action towards the economic segment in which consumer spending is high, such as healthcare, food, and high-tech industries. For further information, cf. FEDERAL TRADE COMMISSION, **Guide to Antitrust Laws – The Enforcers**, https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/enforcers (last visited on May 6, 2021).
[334] FTC Act, §45(a)(1). Herbert Hovenkamp criticizes the use of the term "unfair" in section 5 of the FTC Act, as it recalls business torts practices, which encompasses a set of deceptive and unfair conducts, rather than anti-competitive ones, the Commission's true focus. HOVENKAMP, Herbert, The Federal Trade Commission and the Sherman Act, **Florida Law Review**, v. 62, p. 1–23, 2010, p. 2.
[335] UNITED STATES. USC. Title 15, Ch. 1, §§12-27; Title 29, Ch. 5, §§52-53, Clayton Act. Available at https://www.law.cornell.edu/uscode/text/15/chapter-1.
[336] UNITED STATES. USC. Title 15, Ch. 1, §§1-7, Sherman Act. Available at https://www.law.cornell.edu/uscode/text/15/chapter-1.

Act of 1976,[337] and non-mergers cases, including single-firm conduct, price discrimination, horizontal restraints, and prohibition against unfair methods of competition.

The FTC action in competition matters is procedurally similar to that undertaken in privacy issues. If the Commission has reason to believe that a private party acted unlawfully, it may issue an administrative complaint and initiate a formal procedure before an ALJ or file an action directly before a federal court. In case of presenting a complaint, the decision taken by the ALJ can be appealed to the full Commission, and, eventually, the Commission decision can be contested in the Judiciary in a Court of Appeal. If through investigations the Commission considers that the defendant may have committed a felony, it may refer evidence of criminal antitrust violations to the DOJ. Just as in consumer protection cases, usually, the defendant company reaches an agreement with the FTC through a consent order, so observance of these orders is still important in competition cases, as they will orientate how the Commission will act in subsequent enforcement actions.

Most of the competition actions undertaken by the FTC towards the technology industry involves mergers and acquisitions procedures, encompassing both the Commission's preapproval of societal operations that may harm competition, through its premerger notification program and enforcement actions through which the Agency seek to investigate and challenge those that might lessen competition. Only a few cases refer to non-mergers practices, but all of them investigated unfair methods of competition under section 5 of the FTC Act.[338] Thus, for the purposes of this work, it is worth delving into the FTC's action under Section 7 of the Clayton Act related to its merger and acquisition review and Section 5 of the FTC Act's unfair methods of competition authority.

Just as occurred with deceptive and unfair practices, Congress left to the Commission the definition of unfair methods of competition, for considering that a flexible standard would allow the Agency to reach new practices engaged by business through its case-by-case enforcement. Congress's intent at the time was to complement antitrust law in the United States filling eventual gaps left by the two other antitrust statutes and to enact a regulation whose

[337] Clayton Act, §18a. The premerger notification program requires advance notice of large mergers and acquisitions to both the FTC and the DOJ. The goal is to avoid enforcement costs that both the agencies would face if they had to face consumed anticompetitive mergers or acquisitions. For a detailed explanation about the premerger notification program, *see* FEDERAL TRADE COMMISSION. **Premerger Notification Program**. https://www.ftc.gov/enforcement/premerger-notification-program. Last access on May 06, 2021.

[338] According to advanced search results at the FTC website, the Commission filed, until May 2021, seventeen enforcement nonmerger cases related to the technology industry. Under the "technology industry" the FTC encompasses cable TV, hardware, patents and intellectual property, and software and databases. *See* FEDERAL TRADE COMMISSION, **Cases and Proceedings: Advanced Search**, https://bit.ly/3erslgc (last visited on May 7, 2021).

eventual sanctions would not be as heavy-handed as those depicted in the Sherman Act.[339] Additionally, the Supreme Court has given broad interpretation for section 5 unfair methods of competition, encompassing not only conducts forbidden by the Sherman Act and the Clayton Act, but also those that would 'violate the spirit of these laws'.[340] Thus, even though the FTC did not properly enforce the Sherman Act, it could investigate actions and practices that in abstract violate the Sherman Act as well as conducts that do not fit exactly in the Sherman Act but remains in a penumbra zone. Hovenkamp lists some conducts that are not covered either for the Sherman Act or the Clayton Act, but have the potential to inflict harms to competition, such as monopolies in its incipiency, cartel-like behaviors not encompassed by §1 of the Sherman Act, and prohibition against conducts analogous to abuse of dominant position,[341] including deceptive, collusive, coercive, predatory, unethical, or exclusionary conduct or any conduct that may cause actual or incipient harm to competition.[342]

Despite such broad mandate, for decades throughout the twentieth century, section 5 of the FTC Act played a small role in the United States' antitrust system, which is credited to the concomitant open-ended interpretation of the Sherman Act and the Clayton Act developed by courts at that time, so prosecution usually would occur under one of these two statutes. [343] Indeed, courts were more comfortable in applying antitrust statutes rather than the FTC Act, or the section 5 of the FTC associated with them, rather than a "stand-alone" complaint regarding unfair methods of competition, given the flexibility of these statutes and the lack of development of limiting principles regarding Section 5 by the Commission.[344] However, with

---

[339] FEDERAL TRADE COMMISSION. **Statement of Enforcement Principles Regarding "Unfair Methods of Competition" Under Section 5 of the FTC Act.** Washington, Aug. 13, 2015. Available at https://www.ftc.gov/system/files/documents/public_statements/735201/150813section5enforcement.pdf.

[340] *See* FTC v. Sperry & Hutchinson 405 U.S. 233, 239-244 (1972); F.T.C. v. Ind. Fed'n of Dentists, 476 U.S. 477, 454 (1986) ("The standard of "unfairness" under the FTC Act is, by necessity, an elusive one, encompassing not only practices that violate the Sherman Act and the other antitrust laws, (…) but also practices that the Commission determines are against public policy for other reasons"); *See also FTC v. Raladam Co.,* 283 U. S. 643 (1931) ("that the word 'competition' imports the existence of present or potential competitors, and the unfair methods must be such as injuriously affect or tend thus to affect the business of these competitors -- that is to say, the trader whose methods are assailed as unfair must have present or potential rivals in trade whose business will be or is likely to be lessened or otherwise injured. It is that condition of affairs which the Commission is given power to correct, and it is against that condition of affairs, and not some other, that the Commission is authorized to protect the public. . . . If broader powers are desirable, they must be conferred by Congress").

[341] HOVENKAMP, op. cit.

[342] FEDERAL TRADE COMMISSION. **In the Matter of Intel Corp.** Docket No. 9341, File No. 0610247, Dec. 16, 2009 (Complaint). Available at https://www.ftc.gov/enforcement/cases-proceedings/061-0247/intel-corporation-matter.

[343] KOVACIC, William E .; WINERMAN, Marc, Competition policy and the application of section 5 of the Federal Trade Commission Act, **Antitrust Law Journal**, v. 76, n. 3, p. 929–950, 2010.

[344]Consider, for instance, that the Commission's Statement of Enforcement Principles Regarding "Unfair Methods of Competition" Under Section 5 of the FTC Act was enacted only on August 13, 2015, whereas the Policy Statement on Unfairness was released on December 17, 1980, and the Policy Statement on Deception on October 14, 1983. Cf. *also* FEDERAL TRADE COMMISSION. **In the matter of Intel Corp.** Docket No.

the narrowing of the antitrust interpretation reach by courts, particularly the jurisprudence regarding dominant firms and application of section 2 of the Sherman Act, captained by the influence of Chicago School, and the fear of possible collateral consequences such as damages awards, costly jury trials, some potentially harmful anticompetitive conducts received a "free pass" under antitrust common law.[345] As consequence, "stand-alone" violations of section 5 of the FTC Act have provided an attainable solution.[346] Some commissioners have expressed in their statements concerns regarding a "stand-alone" over-enforcement of Section 5 of the FTC Act, given the lack of clear guidance provided by the Commission and the existence of limiting principles.[347] On the other hand, Tim Wu and Terrell Sweeny consider that the Commission has taken in the last decades a self-restrained approach, probably due to concerns regarding the enforcement of false positives, leading to firms to curb innovation and try new business models.[348]

This limited approach, though, has helped to better define the boundaries and scope of unfair methods of competitions to a set of cases "*where the conduct is very problematic and the harm to the competitive process is very clear*".[349] A process that, he claims, has culminated in 2015 in the issuance of the Statement of Enforcement Principles Regarding "Unfair Methods of Competition" Under Section 5 of the FTC Act.[350]

9341, File No. 061 0247, Dec 16, 2009. (Statement of Chairman Leibowitz and Commissioner Rosch) https://www.ftc.gov/public-statements/2009/12/statement-chairman-leibowitz-commissioner-rosch-matter-intel-corporation.

[345] *Ibid*; KOVACIC, William E .; WINERMAN, op. cit.

[346] KOVACIC; WINERMAN, Competition policy and the application of section 5 of the Federal Trade Commission Act.

[347] *See*, as e.g., Dissenting Statement of Commissioner William E. Kovacic in FEDERAL TRADE COMMISSION. ***In re*** **Negotiated Data Solutions LLC**, File No. 051-0094, at 2-3 (Jan. 23, 2008); Concurring and Dissenting Statement of Commissioner J. Thomas Rosch regarding Google's Search Practices in **In the Matter of Google Inc.** File No. 111-0163 (Jan. 3, 2012); Dissenting Statement of Commissioner Maureen K. Ohlkausen in **In the Matter of Motorola Mobility LLC and Google, Inc.**, Docket No. 1210120, at 1-3 (January 3, 2013).

[348] WU, Tim, **Section 5 and 'unfair methods of competition': protecting competition or increasing uncertainty?**, Columbia Law & Economics Working Paper No. 542; Columbia Public Law Research Paper No. 14-508, 2016, Available at: https://scholarship.law.columbia.edu/faculty_scholarship/1961; MCSWEENY, Terrell, FTC 2.0: keeping the pace with online platforms, **Berkley Technology Law Journal**, v. 32, p. 1027–1050, 2017.

[349] WU, Tim, op. cit., 2016, at 4.

[350] In deciding whether a practice constitutes an unfair method of competition, the FTC will be guided the Commission will be guided by the public policy underlying the antitrust laws, namely, the promotion of consumer welfare; the act or practice will be evaluated under a framework similar to the rule of reason, that is, an act or practice challenged by the Commission must cause, or be likely to cause, harm to competition or the competitive process, taking into account any associated cognizable efficiencies and business justifications; and the Commission is less likely to challenge an act or practice as an unfair method of competition on a standalone basis if enforcement of the Sherman or Clayton Act is sufficient to address the competitive harm arising from the act or practice. FEDERAL TRADE COMMISSION, op. cit., 2015.

The FTC has relied on Section 5 enforcement, for instance, to condemn businesses that have undertaken abusive conducts related to standard-setting and intellectual property that would inflict harm to competition. The existence of technological standards is important to confer interoperability between different ranges of products and promote consumer welfare. However, the adoption of a patent technology as a standard can grant substantial market power to the patent holder, as the other companies in the market will have to adjust to that standard, making investments and eventually facing considerable switching costs, what can lead to an entire industry lock-in.[351] Therefore, to prevent abuses, the patent holder company usually must comply with a series of commitments. The breach of such commitments has been identified as a violation of Section 5 of the FTC Act.

For instance, In *In the matter of Dell Computer Corp.*, the FTC issued a complaint against Dell, a computer technology company, which at that time was a member of a non-profit standards-setting association of hardware and software manufacturers.[352] The association designed a standard for computer hardware named "VL-Bus", having Dell participated in the process, and stated that the standards did not violate any of the company's intellectual property. However, after the VL-Bus has become widespread in the market, Dell informed that the new standard violated one of its patents rights registered one year earlier.[353] Similarly, in *In the Matter of Negotiated Data Solutions LLC*, N-Data acquired patent rights over a new computer networking technology, “NWay", from another company named National Semiconductor, that had previously taken part in a standard-setting organization and with which it agreed to license NWay for a one-time fee of thousand dollars.[354] However, despite the agreement between National and N-Data that the latter would continue to honor the license commitments, N-Data breached the licensing agreement, turning the process substantially more costly.[355] The situation got particularly sensitive because the NWay was the technology compatible with a then-new standard that was widely adopted in the marketplace.

In both cases, the Commission considered that the Defendants' abusive conducts in the management of intellectual property rights would pose harm to competition on computer and

[351] FEDERAL TRADE COMMISSION. **In the Matter of Motorola Mobility LLC and Google Inc.**, Docket No. C-4410, File No. 1210120, Jan. 3, 2013 (Complaint). Available at https://www.ftc.gov/enforcement/cases-proceedings/1210120/motorola-mobility-llc-google-inc-matter.
[352] FEDERAL TRADE COMMISSION. **In the Matter of Dell Computer Corp.** Docket No. C-3658, File No. 931 0097, May 20, 1996. (Complaint). Available at https://www.ftc.gov/enforcement/cases-proceedings/931-0097/dell-computer-corporation.
[353] Id.
[354] FEDERAL TRADE COMMISSION. ***In re* Negotiated Data Solutions LLC**.
[355] Id.

telecommunications industry that trusted the adoption of standards in previous terms, as well as the spread of uncertainty revolving the acceptance of the design standard and, ultimately, the participation in industry standard-setting efforts and the innovation incentives. The FTC has also prosecuted dominant suppliers of electronic components for the practice of exclusionary conducts to cripple rivals or impede the ascent of potential rivals. In *In the Matter of Intel Inc.*, the Commission considered that Intel, a worldwide leader chip maker, engaged in a series to impede its customers, computer manufacturers, to purchase non-Intel computer chips.[356] For instance, considering that Intel was the only company with a strong capability to supply the largest computer makers, it threatened these companies with retaliation if they purchase too many non-Intel CPUs. Besides, Intel also secretly redesigned its key software so that when associated with non-Intel CPU chips, computers would have worse performance.

If the FTC has filed, in the last decade, a couple of complaints targeting digital platforms in matters of online privacy, and has expanded its authority in this realm, the same has not occurred in the competition field. The Commission staff indeed attempted in 2011, when it opened an antitrust probe against Google to inspect both an allegation of breaching its commitments to standard-setting organizations and of "search bias", having decided to settle the first and close the latter.[357] The FTC aimed to assess whether changes in Google's search results page were harmful to competitors, particularly vertical search engines.[358] Google is considered a horizontal search engine, what means that its search results are comprehensive and try to cover any result related to a search query, while vertical search engines focus on a specific category of contents, such as shopping or traveling. Vertical search engines denounced that Google introduced a "Universal Search" results page and, because of that, these vertical search websites were removed from its first page, while highlighting Google's services, and that Google took content from rival companies – e.g. reviews from restaurants and consumer products – for use in its own service without proper compensation, a practice called "scraping".[359]

---

[356] FEDERAL TRADE COMMISSION. **In the Matter of Intel Corp.**

[357] The FTC conducted an investigation against Google in which it analyzed the company's search practices as well as anti-competitive practices related to standard-essential patents undertaken by Motorola, a wholly-owned subsidiary of Google. The FTC issued a complaint in the latter and settle with both Motorola and Google. *See* FEDERAL TRADE COMMISSION. **In the Matter of Motorola Mobility LLC, and Google Inc.** Notwithstanding, this case particularly does not involve Google's platform services, but cellular wireless communication standards.

[358] FEDERAL TRADE COMMISSION. **In the Matter of Google Inc**., File No. 111-0163 Jan. 3, 2013 (Statement of the Federal Trade Commission Regarding Google's Search Practices) Available at https://www.ftc.gov/public-statements/2013/01/statement-federal-trade-commission-regarding-googles-search-practices.

[359] WYATT, Edward. A Victory for Google as FTC takes no formal steps. **New York Times**, Jan 3, 2013. Available at https://www.nytimes.com/2013/01/04/technology/google-agrees-to-changes-in-search-ending-us-

A unanimous Commission considered that Google adopted some design changes of its search results, which led to a negative impact over its competitors, but such impact was not purposeful, as those changes occurred in order to increase the quality of Google's product and improve consumers' experience.[360] Therefore, the eventual negative impact on competitors, in the Commission's view, was related more to Google's 'competitive merits' than with anticompetitive practices. The FTC also extracted from Google a voluntary commitment to remove restrictions on the use of AdWords that would make it more complex for advertisers to manage their ad campaigns across competing platforms, and stop taking its competitor's content, a practice that Commissioner Leibowitz, the FTC chairman at the time, stated as "*the most troubling of its business practices related to search and search advertising*". [361] This outcome allowed Google to solidify its position as a dominant player on the Internet, and to avoid a groundbreaking – and probably costly and lengthy – antitrust action like the Microsoft case in the 1990s, through which the software company was accused of illegally bundling its web browser Internet Explorer with Windows operating system, causing harm to competitors' browsers. Since the DOJ's action against Microsoft, though, there have been no "big antitrust lawsuits" against tech giants – until 2020, when the FTC filed a complaint against Facebook.[362] In fact, FTC commissioners have been conservative about strong regulatory interventions in Internet-based services, given the fast pace of high-tech industries, constant concern about market changes during the investigations, and possible impacts over innovation process and economic growth. [363] The apparently low barriers to entry in the Internet services marketplace,

antitrust-inquiry.html; ROMM, Tony, Google dodges bullet in FTC probe, **Politico**, Jan 3, 2013. Available at https://www.politico.com/story/2013/01/google-dodges-bullet-as-ftc-closes-probe-085724.

[360] FEDERAL TRADE COMMISSION. **In the Matter of Google Inc.** (Statement of the Federal Trade Commission Regarding Google's Search Practices). Available at https://www.ftc.gov/public-statements/2013/01/statement-federal-trade-commission-regarding-googles-search-practices.

[361] WYATT, op. cit.; FEDERAL TRADE COMMISSION. **Google Agrees to Change Its Business Practices to Resolve FTC Competition Concerns In the Markets for Devices Like Smart Phones, Games and Tablets, and in Online Search.** Jan 3, 2013. Available at https://www.ftc.gov/news-events/press-releases/2013/01/google-agrees-change-its-business-practices-resolve-ftc.

[362] The complaint against Facebook will be analyzed in more detail in the next chapter.

[363] FEDERAL TRADE COMMISSION. **In the matter of Google Inc.** File No. 111-0163 Jan. 3, 2013. (Statement of Commissioner Maureen K. Ohlhausen) Available at https://www.ftc.gov/public-statements/2013/01/separate-statement-commissioner-maureen-ohlhausen-matter-google-inc. ("Technology industries are notoriously fast-paced, particularly industries involving the Internet. Poor or misguided antitrust enforcement action in such industries can have detrimental and long-lasting effects. This agency has undertaken significant efforts to develop and maintain a nuanced understanding of the technology sector and to incorporate an awareness of the rapidly evolving business environment into its decisions. The decision to close the search preferencing part of this investigation, in my view, is evidence that this agency understands the need to tread carefully in the Internet space"); In the matter of Google, Inc. (Concurring and Dissenting Statement of Commissioner J. Thomas Rosch regarding Google's search practices) ("I am concerned that imposing a duty on monopolists to allow their customers to interoperate and share data with rivals could discourage innovation, particularly in the software industry").

with fresh startups up with groundbreaking services fast-growing and menacing incumbent firms led many to think "in cyberspace, there could be no such a thing as a lasting monopoly".[364] However, it did not turn out to be true over time. The case against Microsoft, although has not led to the company's breakup, gave room to emerging tech players, such as Google, Facebook, and Amazon, which ironically now have a gatekeeping position on the Internet, controlling a significant amount of information flows on this space.[365]

Conservative positions in the competition realm were not restricted to investigation openings based on unfair methods of competition. Under Section 7 of the Clayton Act, the FTC has the authority to investigate and review mergers and acquisitions. If the Commission concludes that the transaction is likely to harm competition and affect consumers, it can file a complaint before a federal district court under Section 15 of the Clayton Act. However, while performing its mergers and acquisitions review, the FTC adopted a loose position towards digital platforms, being the most significant cases Google's acquisition of DoubleClick, a company that operates in the online advertisement market, and Facebook's acquisition of WhatsApp and Instagram, both applications for social interaction. Those cases raised questions about implications for privacy when the platforms involved in the businesses combine their datasets, giving access to personal information to an entity with which users did not choose to interact with or leading to new combinations and methods of processing data, and consequently, new insights about individual consumers.[366]

There are no FTC public documents related to Facebook acquisition of Instagram and WhatsApp, which makes it a tough job to investigate the reasons that led the Commission to reach the conclusion that such acquisitions would not potentially represent a threat to the social network's market.[367] In 2012, Instagram particularly was a rising direct competitor of Mark Zuckerberg's company and was seen as a serious potential threat to Facebook's business given its friendly functionalities to share photos through mobile phones.[368] Besides, with the acquisition of Instagram, Facebook would be able to bolster its mobile strategy as well as

[364] WU, Tim, op. cit., 2018, p. 120.
[365] Ibid, p. 98.
[366] OKULIAR, Alexander P.; OHLHAUSEN, Maureen K., Competition, consumer protection, and the right [approach] to privacy, **Antitrust Law Journal**, v. 80, n. 1, p. 121–156, 2015, p. 132.
[367] Years later, in 2020, the FTC filed a complaint challenging Facebook's acquisition of Instagram and WhatsApp. This issue will be explored in greater depth in chapter three.
[368] RUSLI, Evelyn M. Facebook buys Instagram for $1 Billion, Dealbook. **New York Times,** [New York], Apr. 9 2012. Available at https://dealbook.nytimes.com/2012/04/09/facebook-buys-instagram-for-1-billion/; CARLSON, Nicholas. Here's the biggest threat to Facebook, and what Facebook is doing about it. **Business Insider**, [s.l.] Feb. 6, 2012. Available at https://www.businessinsider.com/heres-the-biggest-threat-to-facebook-and-what-facebook-is-doing-about-it-2012-2.

combating Twitter and Google+. Two years later, in 2014, Facebook undertook a new step with the purchase of WhatsApp for the record-breaking value of $19 billion. By that time, Facebook's Messenger was the second most used messaging app for mobile devices, only behind WhatsApp. The only public word of the FTC regarding this business refers to a letter sent to Facebook and WhatsApp in which the Director of the Bureau of Consumer Protection express concerns regarding the protection of consumer's privacy in WhatsApp, as the messaging app's privacy policy was far more rigorous in the collection and use of data than Facebook's.[369] The BCP urged both companies to honor the privacy promises made when the acquisition was publicized, and recalled that it has brought many privacy cases related to broken promises of privacy under Section 5 of the FTC Act.[370] Not a word of the Commission regarding possible effects on messaging apps market competition.

It was in the Google/DoubleClick case in which privacy concerns related to access to data appeared more directly in antitrust analysis. DoubleClick was an online advertising company leader in display ads, consisting of images or videos that appear when one visits a website, a type of advertisement Google was not particularly strong.[371] DoubleClick also dominated a technology known as "ad serving", which helped ad buyers to target potential customers and assess whether the ads have performed well, and funnel the advertising of its clients to an ad network, such as Google's AdSense.[372] On the other hand, Google by the time had made most of its revenue from search and contextual ads (ads on a search engine's search result page), has since then dominated that market, but the lack of expertise with display ads made it difficult to attract big brand advertisers.[373] Commenters had raised concerns not only about the potential effects to competitors in the online advertising market but also the threats to consumers' privacy, considering the significant accumulation of data such operation could cause.[374]

---

[369] FEDERAL TRADE COMMISSION. **Letter from Jessica L. Rich, Director of the Federal Trade Commission Bureau of Consumer Protection to Erin Egan, Chief Privacy Officer, Facebook, and to Anne Hoge, General Counsel, WhatsApp Inc.** Apr. 10, 2014. Available at https://www.ftc.gov/public-statements/2014/04/letter-jessica-l-rich-director-federal-trade-commission-bureau-consumer.

[370] Ibid.

[371] STORY, Louise and HELFT, Miguel, Google buys DoubleClick for $3.1 billion, **New York Times**, [New York], Apr 14 2007. Available at https://www.nytimes.com/2007/04/14/technology/14DoubleClick.html.

[372] LAWSKY, David. Google closes DoubleClick merger after EU approval, **Reuters** [s.l.], Mar. 11 2008. Available at https://www.reuters.com/article/us-google-doubleclick-eu-idUSBFA00058020080311.

[373] YIU, Tony, Why did Google buy DoubleClick?, **Towards Data Science** [s.l.] May 6 2020. Available at https://towardsdatascience.com/why-did-google-buy-doubleclick-22e706e1fb07.

[374] ROSENCRANCE, Linda. Privacy groups say Google Double-Click merger will hurt consumers. **Computer World**, [s.l.] Dec 20 2007. Available at https://www.computerworld.com/article/2538252/privacy-groups-say-google-doubleclick-merger-will-hurt-consumers.html; ELECTRONIC PRIVACY INFORMATION CENTER.

After months of investigation, the FTC concluded that Google's acquisition of DoubleClick was unlikely to threaten competition, as the two companies were not direct competitors, and their advertisers served different purposes, with one's price not constraining the other's.[375] The Commission also did not find evidence that the operation would impose harm to its competitors, as the online advertising market was fragmented, and likely to increase and quickly evolve in the next years.[376] Regarding the privacy concerns arising from the merger, the FTC contended, "the sole purpose of federal antitrust review of mergers and acquisitions is to identify and remedy transactions that harm competition. (…) regulating the privacy requirements of just one company could itself pose a serious detriment to competition in this vast and rapidly evolving industry".[377] Besides, the Commission considered that evidence did not indicate that the fusion of Google's and DoubleClick's datasets would be an essential input to success in the online advertising market, as other companies such as Yahoo!, Microsoft, and Time Warner had their own unique datasets appeared to be well-positioned to compete with Google.[378]

However, that was not a unanimous position. Foreseeing some of the possible impacts of concentration of large datasets in the hands of few companies, Commissioner Pamela Harbour, in her dissenting statement reflected on the necessity of a differentiated competitive analysis of data driven-markets. She argued that the acquisition of DoubleClick by Google represented not only a combination of the two firm's products and services, but two significant databases about consumer behavior on the Internet, causing impact in both competition and consumer protection.[379] Through the acquisition of DoubleClick database, Google would exacerbate network effects, with an acceleration of convergence between search and display advertising.[380] Google will be able to match its search results data with browsing information collected by DoubleClick and maximize target advertisement, but the effects on competition in the online advertisement market.[381] Although acknowledging that behavioral advertising

---

Complaint and Request for Injunction, Google & DoubleClick, Inc. [Washington], Apr. 20 2007, p. 2. Available at epic.org/privacy/ftc/google/epic_complaint.pdf.

[375] FEDERAL TRADE COMMISSION. **Google/DoubleClick.** File No. 071-0170, Dec. 20, 2007. (Statement of Federal Trade Commission), Available at https://www.ftc.gov/public-statements/2007/12/statement-federal-trade-commission-concerning-googledoubleclick.

[376] Id.

[377] Ibid., p. 2.

[378] Ibid., p. 12-13.

[379] FEDERAL TRADE COMMISSION. **Google/DoubleClick**, File No. 071-0170 Dec. 20, 2007. (Dissenting Statement of Commissioner Pamela Jones Harbour), Available at https://www.ftc.gov/public-statements/2007/12/dissenting-statement-commissioner-harbour-matter-googledoubleclick.

[380] Ibid., p. 5.

[381] Ibid., p. 8.

creates efficiencies, Commissioner Harbour expressed concerns about relegating data issues to the consumer protection side of the Agency as well as about the intent of the two companies in regards to their data troves.[382]

Commissioner Habour also expressed apprehension regarding the possible outcomes of DoubleClick acquisition for consumer privacy, as it fails to capture the interests of all relevant parties.[383] As seen previously, platforms operate in two or multi-sided markets, so antitrust analysis must take into account all sides of the market. Consumers' side tends to be neglected because the service is often offered free. However, it does not mean that the transaction is costless, as users barter those services for attention and personal data. Thus, if, on one hand, more data gathering would mean more personalization, on the other it would also raise privacy risks. Despite these reflections, Commissioner Harbour agreed with the majority that a privacy-based analysis in an antitrust case would be undesirable, considering that "while this transaction sparked great interest in privacy issues and created momentum for a meaningful discussion, it would be short-sighted to focus on the behavior of a single company (in a merger context) when the issue is relevant to so many other firms as well".[384]

Commissioner Habour's concerns regarding adequate attention of data integration, network effects in multi-sided, and its implications to antitrust analysis remain actual and necessary yet. Theorists have discussed the role of antitrust analysis in the potential harms resulting from data concentration. Some advocate for broader enforcement, even encompassing standards such as privacy, while others consider that antitrust law should not address such risks, being consumer protection the proper path to enforce those harms. In fact, control over digital markets is one of the sources of platforms' power.[385] Network effects, as seen in the previous chapters, foster the rise of online gatekeepers that can take advantage of their privileged position in the networks and restrain the activity of potential rivals through exclusionary conducts.[386]Among other acts or practices, gatekeeper platforms can engage in the following abusive conducts:

> "Those in control of a key platform (such as a mobile phone operating system, leading search engine, or leading online platform) can engage in cheap exclusion. This may include steering users and advertisers to the provider's own products and services to

[382] Ibid. at 9.
[383] Ibid. at 9-10.
[384] Ibid. p. 10.
[385] FUKUYAMA *et al*, op. cit, p. 19.
[386] EZRACHI, Ariel; STUCKE. Maurice E., eDistortions: how data-opolies are dissipating the Internet's potential. **Promarket.** [s.l.], Mar. 27 2018. Available at https://promarket.org/2018/03/27/edistortions-data-opolies-dissipating-internets-potential/; STUCKE; GRUNES, op. cit. ("To maintain its competitive advantage, the company may be tempted to prevent smaller rivals and potential entrants from accessing such data, which might be exclusionary under the antitrust laws").

> the detriment of rival sellers on its platform (and contrary to consumers' wishes); degrading the independent app's functionality, or reducing traffic to the independent app by making it harder to find on its search engine or app store."[387]

Then, it would be legitimate to block mergers and acquisitions or break up them based on the potential harms derived from data concentration and substantial loss of competition.[388] Opponents of such approach, though, tend to consider the elimination of potential rivals through merger operations as too speculative.[389] In addition, they claim that network effects do not necessarily lead to anticompetitive harms or loss of competition.[390] In the social network market, for instance, Friendster was replaced by MySpace, which now was surpassed by Facebook. However, it is undeniable that Facebook engaged in a series of acquisitions through vertical and horizontal integration in the last years, allowing the same conglomerate to offer a range of different services. Giving away Facebook services means to exit two leading social networks (Facebook and Instagram) and two leader messaging services (Messenger and WhatsApp).

Enthusiasts of a Big Data analysis through antitrust lens also claim that data concentration can lead to a loss of quality in the services provided, which would include adequate levels of privacy protection.[391] Difficulties associated with access to data would impede smaller services to improve their products, whereas incumbent platforms would not have incentives to innovate. As smaller platforms providers cannot afford competitive products, it does not prevent incumbent ones from lower their costs and expand their profits on the paid side. Critics contend that, apart from its lack of real-world evidence, potential degradation in the quality of incumbent platforms, but which is still superior to its competitors, is not an antitrust concern.[392] Indeed, antitrust regulators hardly would have the proper means to assess whether there was a quality of the "best search results" or the "best e-commerce". James Cooper argues that platforms incur significant costs to collect, store and process data, so it seems reasonable that they would have afforded such infrastructure without using these outcomes to improve their services.[393]

---

[387] EZRACHI, Ariel; STUCKE, op. cit.
[388] WU, op. cit., p. 128.
[389] Id.
[390] SOKOL, D Daniel; COMERFORD, Roisin, Antitrust and regulating big data, **George Mason Law Review**, v. 23, n. 5, p. 1129–1161, 2016, p. 1148.
[391] STUCKE; GRUNES, op. cit.; EZRACHI, Ariel; STUCKE, Maurice E., op. cit.
[392] SOKOL; COMERFORD, Antitrust and regulating big data, p. 1142.
[393] COOPER, James C. Privacy and antitrust: underpants gnomes, the first amendment, and subjectivity, **George Mason Law Review**, v. 20, n. 4, p. 1129–1146, 2013, p. 1137.

Similarly, some scholars, such as Ariel Ezrachi, Maurice Stucke, and Peter Swire, have also advocated for the assessment of privacy harms in antitrust analysis. They contend that privacy would be a non-price dimension of competition, such as quality, variety, and innovation, with companies offering different levels of privacy.[394] Thus, the existence of dominant firms in the market deprives consumers' choices about privacy, thus reducing the quality of the service.

Besides, platforms have economic incentives to engage in the accumulation of personal data, so there is no market-based solution for this problem.[395] Opponents of this approach argue this type of business model creates efficiencies and promotes consumer welfare, as consumers have access to higher quality services free, which should be weighted with eventual privacy harms.[396] Platforms have engaged in different functionalities to improve their existing services, occasionally even creating new ones. This is true, but a cost-benefit analysis in a matter of privacy can be obscured due to information asymmetries, so it can be especially difficult for users to make this assessment, particularly when it comes to more systemic damages. On the other hand, the addition of a privacy assessment to antitrust analysis would lead to a higher degree of subjectivity, as there is no solid and objective definition of privacy.[397] As there is no agreement about a 'competitive level of privacy', it would increase the discretionary of regulators' choices and lead to differential treatment among mergers.

The debate about privacy harm as antitrust concerns can be seen in fact part of a broad movement that defends new regard to anticompetitive analysis adequate to the new challenges imposed by the data-driven industry, particularly with regards to the consumer welfare standard. In this sense, some of the theorists that share this view defend that antitrust policy should act more thoroughly on political and social values.[398] Tim Wu, for instance, have advocated that the antitrust analysis should recover the antitrust intended economic and political goals, meaning that "courts should assess whether the targeted conduct is that which "promotes competition or whether it is such as may suppress or even destroy competition", rather than rely

[394] EZRACHI, Ariel; STUCKE, op. cit. ("Leading platforms can depress privacy protection below competitive levels and collect personal data above competitive levels. In heavily concentrated markets, personal data is concentrated in a few firms. Consumers have limited outside options that offer better privacy protection. The collection of too much personal data can be the equivalent of paying an excessive price, but one may question whether it should be viewed as a reward for winning the competitive process); *see also* SWIRE, Peter P., Submitted Testimony to the Federal Trade Commission Behavioral Advertising Town Hall, at 5 (Oct. 18, 2007), available at http://ftc.gov/os/comments/behavioraladvertising/071018peterswire.pdf.
[395] STUCKE; GRUNES, op. cit., p. 8-9.
[396] COOPER, op. cit., p. 1137-1138; OKULIAR; OHLHAUSEN, op. cit., p. 151.
[397] COOPER, Ibid., p. 1144; OKULIAR; OHLHAUSEN, Ibid., p. 151-152.
[398] FUKUYAMA *et al*, op. cit., p. 24.

on consumer welfare standard focused on price effects.[399] The risk of such an approach, though, relates to the lack of clear guidelines to address a plurality of objectives and the balancing between them, which could lead to a crisis of legitimacy.[400]

2.4 CONCLUSIONS OF THE CHAPTER

Legal constructions play an important part in the structuration of informational capitalism. In fact, as stressed by Cohen, if, on one hand, there are political and economic certain realms, such as intellectual property expansion with the growing access to the Internet, on the other, there was strong resistance to tougher regulation. That happened, for instance, with antitrust law in the most recent decades, with the decrease of big cases. At the same time, in the Internet-based industry, there was a clear non-intervention ideology, due to a creed that this was a very dynamic sector, so market forces would rapidly self-corrected any deviation or potential anticompetitive practice, which led to the accumulation of data in the hands of few companies. Such orientation emerges in the FTC's decisions to approve mergers and acquisitions required by big techs such as Google and Facebook. On the other hand, there is a growing understanding that maybe antitrust analysis in data-driven markets requires a differentiated approach, which takes into account the control of a company over access to data as well as the protection of users' privacy rights.

Similarly, despite some congressional initiatives, the United States has not managed to enact an omnibus privacy statute. Notwithstanding, the FTC has emerged in the last two decades as a *de facto* privacy authority based on its authority to combat unfair and deceptive practices. If in the beginning, the majority of the Commission's work was to enforce companies' own privacy policies, it has expanded its field of action and has developed a genuinely common law regime, which indeed makes sense considering the U.S. legal tradition. Perhaps here lies a difficulty to international scholars in the understanding of how the FTC has developed probably the most consistent information privacy regime in the United States. Despite the broad mandate to prosecute unfair and deceptive acts or practices, privacy scholars consider that the FTC has adopted a self-restrained enforcement action, and has only taken action against the most glaring privacy violations.[401] Certainly, the FTC enforcement on privacy issues has been gaining notoriety, but the Commission's action is still worth some improvement.

---

[399] WU, op. cit., 2018, p. 136.
[400] FUKUYAMA *et al*, op. cit.
[401] HARTZOG, Woodrow; SOLOVE, Daniel J, The Scope and Potential of FTC Data Protection, **The George Washington Law Review**, v. 83, n. 6, p. 2230–2300, 2015; HOOFNAGLE, op. cit.

Although recognizing the limitations of the FTC's account, its broad dual mandate depicted in Section 5 of the FTC Act to declare unlawful unfair methods of competition and deceptive and unfair acts or practices affecting consumers positions the Agency in a strategic spot to understand and combat the nefarious effects derived from platform practices. The three complaints against Facebook, which will be better explored in the next chapter, demonstrate that. Investigating in greater depth the case against Facebook is important because it is the first time the FTC is taking action against a big tech corporation in both consumer protection and competition, so they can function as an important indicator about how the Commission is trying to figure out regulatory measures against dominant platforms.

CHAPTER 3 TOWARDS A REGULATION OF PLATFORMS: THE FTC AGAINST FACEBOOK

3.1 THE RISE OF FACEBOOK IN THE SOCIAL NETWORK MARKET

In sixteen years, Facebook has become more than a website on the Internet. With the impressive mark of 1.69 billion users in 2020, the social network turned into an online space where people share their thoughts, connect with friends, negotiate goods and services, plan events, promote causes, and a wide variety of other activities, in line with its mission "to give people the power to build community and bring the world closer together".[402] Facebook as social network is a product of Facebook, Inc. ("Facebook group"), a conglomerate that also owns Instagram, Messenger, WhatsApp, and Facebook Reality Labs and Oculus as its main product, which confers the company an advantageous position in the platform market.[403] On Facebook, in particular, users are encouraged to disclose a vast amount of personal information that otherwise in the offline world people would not open to a stranger, such as educational history, job, favorite movies, favorite music, hometown, sexual orientation, political affiliation, religion and so forth. In the social network, a person can also upload photos, videos, share links to websites, and react to other users' posts through the "like" button. Each user has a User Identification Number ("User ID"), a unique number by which it is possible to obtain profile information from Facebook. All those information taken together is capable to trace very particular aspects of a user's personality traits, likes, and dislikes.

In the Facebook early days, the possibility to configure privacy levels was differential when compared with so-then popular social networks such as MySpace.[404] To make users more comfortable about sharing such kind of information, Facebook offers different layers of privacy, so that users can customize their profiles in the Privacy Settings Page: data that is available to the public, to their friends, and friends of friends. Users could also set up information collected through third-party applications ("Platform Apps"). When a person utilizes one of these apps, they request to collect some personal data from his or her profile and, eventually, from his or her friend list.

---

[402] FACEBOOK. **Company Info**. [Menlo Park], [s.d.] Available at https://about.facebook.com/company-info/ . Last access May 3 2021.

[403] FACEBOOK. **Annual Report 2020 (Form 10-K)**. [Menlo Park], Jan. 28 2021, p. 7. Available at https://investor.fb.com/financials/sec-filings-details/default.aspx?FilingId=14646367. Last access Mar. 20 2021.

[404] SRINIVASAN, Dina. The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy. **Berkeley Business Law Journal**, v. 16, n. 1, p. 39, 2019.

Despite its promise to give users more control over their own information, Facebook's business model relies on heavy collection and processing of data. As a digital platform, Facebook operates in a logic of a two-sided market. The service is offered at no cost to users of the social network and, similar to Google, it relies on its users to generate a vast amount of data and content that are processed by data scientists or algorithms to generate metadata (organized datasets where those companies have worked on) that is sold to advertisers and interested third parties. In a world where attention is scarce and information is abundant, the quantity of persons accessing social networks and the time spent there is a valuable resource to advertisers, who can needle their public precisely through Facebook's complex data processing mechanisms. Currently, the sale of advertisement space on its various social media platforms constitutes nowadays the primary source of Facebook's revenue. Both Google and Facebook indeed control the bulk of the United States digital ad market capturing nearly 56% of the revenues in 2020, although their market share has slightly dropped with the emergence of Amazon.

Along with Google and Amazon, Facebook has emerged as one of the paradigmatic firms of the informational capitalism age. Whereas admired by its innovative business and the creation of one of the greatest networked communities of our times, its transcendental influence over a bulk of urgent questions such as freedom of speech, information control and manipulation, privacy, and democracy. In recent years, the company has faced intense public scrutiny about both its privacy and competition methods, raising the attention of public authorities.[405] The FTC case against Facebook, though, is not that recent, since the Commission filed the first complaint for violation of privacy promises in 2012.

Facebook has endured a long history of privacy violation accusations, as the company systematically launched new features at Facebook and configure them as default options without previously requesting users' consent. In 2007, Facebook launched Beacon, a program that would share automatically into users' News Feed purchases made by them on outside websites, a feature immediately repealed, forcing Mark Zuckerberg to take a step back.[406] Two years later, in 2009, Facebook engaged in successive revisions of its privacy policies and settings either stating that users could not delete their data when they left the social network or making some of the users' profile information public by default.[407] The constant updates in its

[405] For a summary of legal proceedings against Facebook, *see* Facebook, Inc., Annual Report 2020 (Form 10-K), p. 45.
[406] SHIFFMAN, Betsy. Facebook CEO Apologizes, Lets Users Turn Off Beacon. **Wired.** [s.l.] May 12, 2007. Available at https://www.wired.com/2007/12/facebook-ceo-apologizes-lets-users-turn-off-beacon/. Last access May 13, 2021.
[407] SCHONFELD, Erick. **Zuckerberg on who owns user data on Facebook: it's complicated**, **Techcrunch.** [s.l.] Feb. 16, 2009. Available at https://techcrunch.com/2009/02/16/zuckerberg-on-who-owns-user-data-on-

privacy policies and practices not only led to users to confusion but also raise concerns about potential threats.[408] Such circumstances lead a group of public interest organizations to file a complaint against Facebook before the FTC in 2009 contending that then recent changes in Facebook's privacy policies mandating disclosure of information was an unfair practice and that the company's policy regarding data sharing with third-party apps was deceptive.[409] Years later, just after the Cambridge Analytica scandal boomed on the newspapers worldwide, revealing data manipulation practices that went far beyond microtargeting advertisement and presented impact in the U.S. presidential elections in 2016. In this scenario, the FTC filed the second complaint against Facebook and applied the largest fine ever imposed in its history, a five billion dollars penalty.

Meanwhile, Facebook has also faced increased scrutiny about its competition strategy, as evidence has shown that it has systematically maintained its dominant position through the practices of unfair methods and practices. As seen in previous chapters, platform markets, in special social networks markets, tends to suffer network effects. Individuals use social networks to interact with family, friends, and people with whom they share common interests. Thus, when a certain social network becomes popular, there is a tendency of new users of social networks and users of different social networks to migrate to the one popular. In the early 2010s, when social networks were flourishing, Facebook faced competition from companies such as Friendster, MySpace, and Orkut, but prevailed over them.[410] Since then, Facebook has held a comfortable position due to network effects, leading to high barriers to entry of new competitors as well as high switching costs. Certainly, social network services are nonrivalrous, which means that an individual can have different accounts in multiple networks. However, the majority of users is not equally active in all their social networks, thus they tend to access with higher frequency those networks where he or she can find most of their social circle. Besides, platforms are not interoperable, so there is a tendency for users to stick with the most popular one. It does not mean, though, that such circumstances will endure forever.

---

facebook-its-complicated-2/ Last access May 13, 2021; KINCAID, Jaso. The Facebook privacy fiasco begins. **Techcrunch.** [s.l.] Dec. 10, 2009. Available at https://techcrunch.com/2009/12/09/facebook-privacy/. Last access May 13, 2021.

[408] KEYS, Mattew. A brief history of Facebook's ever-changing privacy policies, **Medium.** [s.l.] Mar. 21, 2018, https://medium.com/@matthewkeys/a-brief-history-of-facebooks-ever-changing-privacy-settings-8167dadd3bd0. Last access May 13, 2021.

[409] ELECTRONIC PRIVACY INFORMATION CENTER. **FTC Facebook Settlement**. [Washington], [s.d.]. https://epic.org/privacy/ftc/facebook/. Last visited Mar. 28, 2021.

[410] For explanations about the success of Facebook over other social networks, *see* e.g. PRESS, Gil. Why Facebook triumphed over all other social networks. **Forbes**. [s.l.] Apr. 8, 2018. Available at https://www.forbes.com/sites/gilpress/2018/04/08/why-facebook-triumphed-over-all-other-social-networks/?sh=3e7e3af76e91 . Last access May 13, 2021.

In fact, Mark Zuckerberg was right when he realized that, although Facebook's prevalence probably would not be dethroned by another online service similar to that delivered by its social network, it could happen with the emergence of differentiated online service. That was, indeed, a recurring concern in the company. Internet services market has low set-up costs, economies of scale, and are highly innovative. Nonetheless, Facebook, just as other businesses such as Amazon and Google, grew stronger.[411] In fact, in a ten-year-old period, much of the Internet traffic has become mediated by few big technology firms, Facebook among them. Was Facebook too competent in delivering outstanding quality and innovative services? Inquiries tend to deny it, as Facebook was accused of systematically engaging in anticompetitive conduct, leading the FTC to file a complaint for violation of Section 2 of the Sherman Act and Section 5 of the FTC Act. This considered, the aim of this chapter is to depth into the complaints the FTC filed against Facebook, a leading actor of informational capitalism, and offer a reflection about the regulatory means that the Commission has resorted in the three cases.

3.2 THE FTC AGAINST FACEBOOK

3.2.1 The first complaint against Facebook: frustrated privacy expectations

Facebook's practices of collection and sharing of personal data and its relationship with application companies and advertisers are inherent to the social networks business model. Platforms operate under a data imperative, so their primary goal is to create an environment where people feel comfortable to expose their personal information and spend a considerable amount of time interacting with other users. Nonetheless, if in George Orwell's novel 1984 there was a persistent reminder that Big Brother was watching you, private surveillance undertaken by Facebook and other platforms is typically silent, discrete, unilateral, and unauthorized. To disclose information about themselves, users must have the impression they are in a healthy and safe environment. The creation of a minimally comfortable environment is important not just to incentive the actual users to provide more data, but also to achieve new users. These are one of the main reasons for social networks to adopt community standards forbidding some conduct such as violence, obscenity, and hate speech, as well as privacy settings. They want to have the sensation that is safe to disclose information on the social network giving the potential harms associated with high exposure online. Therefore, to gain their confidence, platforms have to make promises about privacy standards, but these promises are vague, wordy, and sometimes

[411] WU, op. cit., p. 120.

do not reflect the reality of companies' practices. Likewise, notices about any modification of those promises often are concealed by their own unclearness or by architecture.

After more than a year of investigation, the FTC disclosed the first action against Facebook on November 29th, 2011, targeting the sharing of data between Facebook and third-party apps.[412] In the first action towards Facebook, the Commission presented eight counts, mainly focused on the false or misleading promises made by Facebook in its Privacy Policy, especially after the policy changes made in December 2009 (counts 1-3), as well as in the data collection and sharing practices undertaken by third party Apps (counts 4-7). The Commission also presented a charge for violation of the U.S.-E.U. Safe Harbor Framework for data transfer outside of the European Union (count 8). With the complaint, the FTC sought to address a series of Facebook's practices of disclosure and sharing of data as deceptive practices in violation of section 5 of the FTC Act.

As portrayed in the complaint, Facebook users had access to a "Central Privacy Page" where they could configure the type of data shown in their profile, including birth date, education history, bio, games activity, music activity, interests, likes, and so forth, and for who it was shown, *e.g.* "only friends", "friends of friends". Nonetheless, Facebook was not complying with the terms of its privacy policy. The social network's policy had not informed that such information would be accessible not only by third-party apps ran by the individual herself, but also by apps used by her friends ("friends' apps"), which was considering a misleading representation.[413] Secondly, the FTC also considered deceptive the fact that some of these third-party apps were collecting more data than needed to operate, despite Facebook's guarantee that such apps would only access data related or necessary to their purposes.[414] Thirdly, oppositely to Facebook's statements that the social network did not share personal information with third parties without users' prior consent, third-party apps and platform advertisers were capable of accessing such information. Platforms advertisers in special had access to the users' data who clicked on their ads and to whom target advertisements were sent, which allowed them to access an extensive profile of individual users and combine it with browsing information.[415]

[412] FEDERAL TRADE COMMISSION. **In the Matter of Facebook, Inc.** Docket No. C-4365, File No. 0923 184, Nov 29, 2011. (Complaint) Available at https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc.
[413] Ibid, p, 9.
[414] Ibid, p. 10.
[415] Ibid, p. 13.

As seen in the last chapter, the FTC has worked to improve its notice and choice model to analyze deception claims through a broader and contextual approach more focused on consumers' expectations rather than the text of privacy policies. The Commission undertook an analytical comparison between the information provided by the company in different sources - privacy policy, privacy settings webpage, and posts at Facebook's blog - and how indeed Facebook architecture works, expanding its parameters to verify deception. Although still relying on the social network's privacy policies as the main source of its analysis, while investigating Facebook, the FTC has also taken into account the consumer expectations and the influence of computer interfaces on consumer behavior.[416] Besides, the mere general noticing regarding data collection was not enough. Even in situations where the users have awareness of data harvest practices, users should be informed about the type of data collected and the extent to which the collection occurs.[417] This broader interpretation, which does not give great weight to boilerplates terms of contracts, aligns with the FTC's role of protecting consumers against harmful practices, which are the weaker party in a relationship inherently asymmetric.

The Commission also charged Facebook with unfairness, as after privacy changes on Facebook settings occurred in December 2009 the social network made public by default information that was previously restricted by users, without any prior notice. In the Agency view, the practice had the potential to cause substantial injury to users, with unauthorized exposure of sensitive information – political view, sexual orientation - to third parties, such as employers, government organizations, business competitors, or even unwanted contacts.[418] Here, Facebook went beyond Gateway and changed not only its policies but also prior choices users have made on their privacy settings.[419]

As in the vast majority of its activities related to Section 5 enforcement, the FTC and Facebook signed a consent order, an agreement through which Facebook compromised to the obligations imposed by the Commission. The FTC consent orders are relatively standardized, so the duties imposed over Facebook were not particularly different from those previously laid down to other companies investigated by the Commission. With the conclusion of the

---

[416] *See* FEDERAL TRADE COMMISSION. **Google, Inc.**, Docket No. C-4336, File No. 1023136 (Fed. Trade Comm'n October 13, 2011) (complaint), https://www.ftc.gov/enforcement/cases-proceedings/102-3136/google-inc-matter; FEDERAL TRADE COMMISSION. **United States v. Path, Inc.** Case 3:13-cv-0448 (Northern District of Cal. Aug. 2, 2013) (consent decree and order for civil penalties, permanent injunction, and other relief) https://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathincdo.pdf.

[417] FEDERAL TRADE COMMISSION. **In the Matter of Sears Holding Management Corporation** (complaint)**.**

[418] FEDERAL TRADE COMMISSION. **In the Matter of Facebook, Inc.**, p. 9-10. (complaint)

[419] Ibid. at 9.

settlement, Facebook did not have to admit publicly any wrongdoing and agreed to modify its practices, though.[420] Through the order, the Agency forbade Facebook to give misleading information about its privacy or security practices and the extent of user control over privacy settings.[421] Additionally, the order established that, before sharing any information with third parties, Facebook must obtain users' affirmative express consent and make clear to them the type of data, the identity or categories of third parties, and information whether the sharing exceeds the user's privacy settings.[422] Although the FTC decisions have taken into account the whole scenario to assess whether a practice is deceptive, including design choices and statements given by companies, not limited to their privacy policies, the primary goal in this consent order was to impose Facebook compliance with its own privacy statements and give users 'sufficient notice mechanisms', so they could choose what kind of data they permitted to share, rather than impose limits on the collection, transmission of data by Facebook through tougher regulation of its business model. It reflects a conception of privacy based on users' control over their own data.

As seen in the previous chapter, through the notice and choice model, companies are obliged to provide sufficient information for data subjects, for they have the right to consent or not to collection and processing. However, this approach, on which deception analysis relies, has shown itself as problematic in the context of informational capitalism practices. This is because, even when there is proper notice about data collection and use practices, consumers have difficulty assessing the risks and benefits of granting access to their data. There is an intrinsic difficulty of analyze the trade-off between privacy and the convenience provided by technological services and goods.[423] Privacy policies settings can also present a complex language and users do not always have the means to understand and process their terms, and hardly support a rational decision regarding privacy choices.[424]

---

[420] Commissioner J. Thomas Rosch wrote a dissenting statement arguing that defendants, under Section 5 of the FTCA, are not allowed to simultaneously settle the issue and deny the allegations outlined in the complaint. Besides, Commissioner Rosch expressed doubts about whether the Order would cover all deceptive practices related to information sharing practices to third-party apps. FEDERAL TRADE COMMISSION. **In the Matter of Facebook, Inc.,** Docket No. C-4365, File No. 092 3184. (Dissenting Statement of Commissioner J. Thomas Rosch). Available at https://www.ftc.gov/public-statements/2012/08/dissenting-statement-commissioner-j-thomas-rosch-matter-facebook-inc.

[421] FEDERAL TRADE COMMISSION**. In the Matter of Facebook, Inc.,** Docket No. C-4365, File No. 0923 184 August 10, 2012. (decision and order). Available at https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.

[422] Ibid., p.4.

[423] ACQUISTI; GROSSKLAGS, op. cit.

[424] Id.

Even a person who is capable of understanding privacy policies and aware of the risks involved in a privacy transaction does not have entire control over her data will not be able to fully manage her data. Firstly, due to a time-cost problem. Reading all privacy policies would cost an American Internet user 201 hours a year, approximately $3,534.[425] This is not even feasible. Think, for instance, in an individual after a working day that in the evening browsers on the Internet to relax who is faced with tons of cookie settings to accept in every single website she visits. It is unlikely that in all those cases users will grant duly attention to those policies.

Secondly, the notice and choice model does not address the post-transaction harms. If surveillance practices may be limited through restrictions on data collection, it does not prevent other problems associated with data aggregation and algorithmic deduction. Hardly a limitation on information collection alone will assure a greater degree of privacy if aggregation practices remain comprehensive. As Solove points, maybe a piece of information does not tell much about an individual, but with the gathering of many of them will be possible to build a mosaic and get a reasonable portrait of a person.[426] In information capitalism, in a context in which data aggregation and algorithmic-mediated processes grow more sophisticated, permitting achievement of outcomes and correlation in an even shorter period. Platforms have become capable of predict with high accuracy an individual's race, sexual orientation, political preference, or even whether he or she smokes based on their online activity. Based on Facebook Likes of 58,000 volunteers, researchers were capable of reasonably predict whether a person is Christian or Islam (82% of accuracy), whether a man is gay (88% of accuracy), or even if the user's parents separated before he or she turned 21 years old (60% of accuracy). [427] Therefore, it is not impossible that companies know more about a person than it actually disclosed.

Thirdly, notice and choice do not function well in business models that are subject to network effects. As seen in chapter one, there is a growing dependency on platform services. As most of these services are free – or at least reasonably cheaper - and of good quality, they spread across markets and create a large users community in which they share and interact vigorously. Thus, exiting may not be an option, as the social – or even economic – costs will be high. In this sense, users individually do not have proper control over their information

[425] MCDONALD, Aleecia; CRANOR, Lorrie Faith. The Cost of Reading Privacy Policies. **Journal of Law and Policy for the Information Society**, v. 4. N. 3, 543-568, p. 565, 2008.
[426] SOLOVE, **Understanding privacy**.
[427] Kosinski, M.; Stillwell, D.; and Graepel, T., Private traits and attributes are predictable from digital records of human behavior, **Proceedings of the National Academy of Sciences of the United States of America.** [s.l.], 2013. Available at https://doi.org/10.1073/pnas.1218772110.

disclosed, as they will be pushed to accept the Privacy Policy independently of their thoughts. Therefore, reliance on simply restoring users' choice about data management hardly will truly give them autonomy.

In addition to forbidding Facebook to misrepresent its privacy practices to users, the FTC also imposed some monitoring mechanisms over the company.[428] The Commission mandated Facebook to "establish and maintain a comprehensive privacy program" to evaluate privacy risks related to its activities and to protect user's personal information.[429] Additionally, the Commission ordered Facebook to obtain periodical assessments by an independent third-party professional for long terms, usually 20 years,[430] as a mechanism to verify whether the respondent is complying with the agreement. The FTC demanded Facebook the obtainment, in a 20 years period, of an assessment and a report prepared by an impartial third party to evaluate its privacy program, as well as routine submission of a compliance report to the FTC, among other measures.[431]

Since the FTC cannot impose fines for unlawful practices, an important aspect of the FTC consent decrees is the lengthy monitoring term and mandated disclosure imposed to the defendant company for a considerably long period. The subjection to the FTC's higher scrutiny aims to both guarantees that the company will not adopt another deceptive or harmful practice, as well as induce a permanent change in how the business works. As information security and privacy issues are highly complex and the FTC usually lacks the financial and personnel resources to address monitoring procedures, the Commission imposes the delivery of private third-party assessments.[432] Through these assessments, it aims to verify whether the company is complying with its own claims about privacy and information security. However, private monitoring also endures some problems, as the defendant company usually afford the assessments, so the third-party monitoring company usually does not have incentives to push

[428] Rory Van Loo describes regulatory monitoring as "the collection of information that the agency can force a business to provide even without suspecting a particular act of wrongdoing. The two main categories of monitoring are remote report collection and on-site visits", VAN LOO, Rory, The missing regulatory state: monitoring businesses in an age of surveillance, **Vanderbilt Law Review**, v. 72, n. 5, p. 1563–1631, p. 1574, 2019.
[429] FEDERAL TRADE COMMISSION. In the Matter of Facebook, Inc., Docket No. C-4365, File No. 0923 184, Aug. 10, 2012,. (decision and order, p. 5 and 6) Available at https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.
[430] Cf. e.g. FEDERAL TRADE COMMISSION. **In the matter of Snapchat.** Docket No. C-4501, File No. 1323078, Dec. 14 2014. (decision and order, p. 3). Available at https://www.ftc.gov/enforcement/cases-proceedings/132-3078/snapchat-inc-matter; FEDERAL TRADE COMMISSION. **In the matter of Google, Inc.** Docket No. C-4336, File No. 1023136, Oct. 13 2011. (decision and order p. 5). Available at https://www.ftc.gov/enforcement/cases-proceedings/102-3136/google-inc-matter.
[431] Id.
[432] VAN LOO, Rory, op. cit. p. 1600-1601.

too hard and adopt a loose posture.[433] For instance, Google's first privacy assessment had approximately thirty pages, a considerably short number for a company that deals with massive amounts of personal data, and concluded that its privacy controls were operating totally accordingly and effectively.[434] The year after the issuance of the first consent decree, the FTC imposed Google a $22.5 million fine for tracking Apple's Safari browser users. On the other hand, the FTC usually does not publicly disclose these assessments, although one can have access to such assessments through a Freedom of Information Act - FOIA request. Civil society entities and academia have been defending that, in the name of transparency, these assessments proactively should be publicly available by the Commission, a thought that has also already been endorsed by Commission members.[435] The submission of assessment, though, as pointed by Commissioner Slaughter, is only a part of the company's tasks to comply with the FTC order, as FTC's efforts in monitoring also encompass continuous communication between Commission's attorneys and representatives of the nonpublic companies.[436]

Between 2012 and 2018, the FTC did not engage in any additional investigation against Facebook, despite new privacy violation accusations have popped up in the media.[437] However, the scenario changed when Facebook found itself in the eye of a storm due to the Cambridge Analytica revelations involving the U.S. Presidential elections in 2016, facing accusations of data misuse even more serious than those once investigated by the Commission in the past. The worldwide repercussion of the Cambridge Analytica case and the following discussions regarding data manipulation and the future of democracies. Immediately, the FTC felt pressured to give a regulatory response accordingly, imposing the highest fine in its history.

---

[433] Id.

[434] HOOFNAGLE, Chris Jay. Assessing the Federal Trade Commission's privacy assessments. **IEEE Security & Privacy**, v. 14, n. 2, p. 58–64, 2016. Available at https://www.computer.org/cms/Computer.org/ComputingNow/docs/ieeesecurity-and-privacy-assessing-federal-trade-commissions-privacyassessments.pdf.

[435] FEDERAL TRADE COMMISSION. **In the matter of Uber Technologies, Inc.** Docket No. C-4662, File No. 1523054, Oct. 25 2018. (Statement of Comm'r Rebecca Kelly Slaughter, p.3) Available at https://www.ftc.gov/enforcement/cases-proceedings/152-3054/uber-technologies-inc; FEDERAL TRADE COMMISSION. **In the matter of Uber Technologies, Inc.** Docket No. C-4662, File No. 1523054, Oct. 25 2018. (Statement of Comm'r Rohit Chopra). Available at https://www.ftc.gov/enforcement/cases-proceedings/152-3054/uber-technologies-inc.

[436] FEDERAL TRADE COMMISSION. **In the matter of Uber Technologies, Inc.** Docket No. C-4662, File No. 1523054, Oct. 25 2018. (Statement of Comm'r Rebecca Kelly Slaughter, p.3) Available at https://www.ftc.gov/enforcement/cases-proceedings/152-3054/uber-technologies-inc.

[437] *See*, e.g., Facebook's psychological study exposing one group of users to positive emotional content on their News Feed and another group to negative emotional content to analyze whether publications on their feed would induce their posting behavior, without their awareness. MEYER, Robinson. Everything we know about Facebook's secret manipulation experiment. **The Atlantic**. [s.l.], Jun. 28 2014. Available at https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/. Last access Mar. 30, 2021.

Notwithstanding, the case raises questions about the limitations of the Commission's regulatory toolkit and the challenges derived from attempts to regulate online platforms.

3.2.2 The second complaint against Facebook: after Cambridge Analytica

The FTC imposition of a consent order little compelled Facebook to review its privacy policies. Seven years later, the social network saw itself in a scandal involving the data broke the Cambridge Analytica, which raised awareness of the behavior manipulation that could occur due to the use of data and even lead to a distortion of elections results. As broadly reported, Alexandr Kogan, a researcher, developed an app, with Facebook's awareness, called "This Is Your Digital Life" through which around 270,000 Facebook users took a survey for academic use. However, the app collected data not only from its own users but also from users' friends on Facebook, leading Kogan to accumulate data from over 87 million Facebook users. Kogan shared the users' information acquired through the app with Cambridge Analytica, a data analytics and political consulting company. Cambridge Analytica used this great amount of behavioral data accumulated to build user's psychological profiles and analyze their psychological traits. The outcomes of this analysis were used later to offer political consultancy to assist Trump's political campaign to United States 2016 Presidential Election and Brexit Leave campaigners through microtargeting political advertising.

The revelations about Facebook's misuse of data lead the FTC to reopen the investigation against the company and hold it accountable for its failure to comply with the terms of the 2012 Order and the FTC Act. The Commission also opened a separate investigation against Cambridge Analytica and Alexander Kogan for violations of the Privacy Shield.[438] As reported in the Complaint about Civil Penalties, although users could opt-out from Friend's App collection, the path through the social network to manage these settings was obscure and not intuitive.[439] In fact, this control was not only different from that users usually do when they post a photo, a status update, or a video, in which they can choose who can see the information, for example, "Friends" or "Friends of Friends", but even located in a different tab.[440] Thus, to change their settings, users must at first realize that there are two different configurations to

[438] FEDERAL TRADE COMMISSION. **In the matter of Cambridge Analytica, LLC.** Docket No. 9383, File No. 1823107. Available at https://www.ftc.gov/enforcement/cases-proceedings/182-3107/cambridge-analytica-llc-matter.
[439] FEDERAL TRADE COMMISSION. **In the Matter of Facebook, Inc.,** Civil Action No. 19-cv-2184, Apr. 28 2020 (Complaint for Civil Penalties, Injunction, and Other Relief at 17-21) Available at https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf.
[440] Ibid, p. 12-17.

manage the information they shared with their friends and third-party apps in general, so few users opted out of this default setting.[441] Besides, the language of the platform set stated that if the user opted out, she would not be able to use Facebook's integration on third parties apps or websites, but did not disclose properly that Facebook shared profile information with Apps and that setting would prevent such sharing.[442]

Indeed, Facebook was aware of the risks of granting broad data access to third-party apps. Nonetheless, to continue giving access to user's data, the company evaluated how certain apps could be financially beneficial, by either paying for advertisement spaces or offering reciprocal data-sharing arrangements rather than their data management practices.[443] In 2014, two years after the issue of the FTC's consent order, at the F8 conference, Facebook declared that it was not allowing third-party apps to collect personal data about users' friend lists anymore.[444] However, it was later discovered that Facebook still had private arrangements with app developers, referred to as "Whitelisted Developers", to collect data from app users' friend list. Thus, despite Facebook's public speech that the platform was removing access to Facebook friends' data, it secretly continued to grant broad access to a group of developers to Whitelisted Developers, which included dating apps, retail, and technology companies.[445] Facebook also acted recklessly by granting access to app developers to Facebook users' data, insofar as the company did not review the apps' privacy policies and only demanded a declaration that they would comply with Facebook's policies and conditions, and has never enforced its data-sharing policies thoroughly.[446] The FTC also accused Facebook of failing to provide adequate information about sharing users' mobile phone numbers for advertising and about the existence of a face recognition setting for millions of Facebook users in the U.S.

After a thorough investigation, Facebook and the FTC agreed to enter a Stipulated Order for Civil Penalty, Monetary Judgement, and Injunctive Relief ("Stipulated Order") in which the social network was ordered to pay five billion dollars civil penalty. In line with the 2012 Order, the Commission maintained Facebook's prohibition to misrepresent the extent to which it maintains data privacy and security and to obtain users' express and clear consent prior to sharing any personal information with third parties that exceeds the restrictions imposed in the

[441] Ibid, p. 20.
[442] Ibid, p. 21.
[443] Ibid, p. 28.
[444] Ibid, p. 29-30.
[445] Ibid, p. 33.
[446] Ibid, p. 34- 36.

User's Privacy Settings.[447] Additionally, the Commission ordered Facebook to erase from its servers information previously deleted by users, with few exceptions, such as to prevention of fraud and malicious activity, as well as to limit third party access to users' deleted data.[448] The FTC also mandated Facebook to implement stronger governance and compliance measures in comparison with the 2012 Order. The Commission established more detailed privacy program requirements, including a risk assessment, regular privacy training programs for the company's employees, and the description of the procedures to implement the privacy program.[449] The imposition of such obligations by the FTC is unprecedented and probably will influence subsequent cases. Similarly, the Commission enhanced the biannual privacy program assessments. The FTC also imposed new obligations to Facebook, including a warning about the occurrence of the covered incident in 30 days, the installation of an independent privacy committee with independent members; submission of quarterly certifications that the company complies with its privacy program; establishment of new tools for the Commission investigate compliance.[450]

The majority opinion, which authorized the Stipulated Order, announced it as "*a historic victory for American consumers*", stressing that, for its value and breadth, this was a landmark penalty, with the implementation of dramatic changes on Facebook's internal policies related to privacy and increase level of transparency.[451] Certainly, the measures imposed by the Commission are comprehensive and on some levels unprecedented. It will take some time to verify whether those measures have worked or not. For now, however, the Facebook case exposes some of the difficulties and limitations of the *ex-post* case-by-case regulatory model developed by the Commission to address privacy damages incurred by big technology companies. Although the Commission has imposed the ever-largest fine in its history and bulk of obligations, this was the second investigation against Facebook. The facts depicted in the complaint became known due to the Cambridge Analytica outbreak, exposed by the media in a denounce of one of its employees, not properly through monitoring mechanisms implemented by the Commission in the 2012 Order.

[447] FEDERAL TRADE COMMISSION. **In the Matter of Facebook, Inc.** Docket No. C-4365, File No. 1823109, Apr. 28, 2020. (Decision and Order, p. 5) Available at https://www.ftc.gov/system/files/documents/cases/c4365facebookmodifyingorder.pdf.
[448] Ibid. at 6.
[449] Ibid. at 8-12.
[450] Id.
[451] FEDERAL TRADE COMMISSION. **In the Matter of Facebook, Inc.** Docket No. C-4365, File No. 1823109, July 29 2020. (Statement of Chairman Joe Simons and Commissioners Noah Joshua Phillips and Christine S. Wilson). Available at https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc.

As seen in the first chapter of this work, Zuboff calls the 'dispossession cycle' the set of operations, which includes administrative, technical, and material capabilities divided into four cycles: incursion, habituation, adaptation, and redirection.[452] Incursion occurs with the invasion of the private spaces of everyday life (laptops, mobile phones, TVs, watches), whereas habituation refers to the temporal dysfunction between regulatory institutions (agencies, Congress, courts), which follow a slow pace, and platforms, whose practices are rapidly changed, leading users to perceive the intrusion as normal, helpless.[453] When regulatory authorities finally have the means to target them, then it comes the third stage of the cycle, adaptations when companies comply with the orders of the governmental authorities; then, in the final stage, redirection, although the companies seem to adhere to the regulator's order, with new rhetoric and rebranding, they redesign their practices to go back to their previous operation, but in a new and more subtle fashion.[454]

The two cases against Facebook reflect quite well this cycle. Facebook's *incursion* towards behavioral data begins stimulating people to voluntarily share their personal information, interests, and thoughts as much as possible because it is that variety of information and users that make a social network valuable. The more interactions through the platform, the greater and varied is the information that Facebook can collect, analyze, deduce. As seen previously, users usually neither have knowledge of the potential impacts of surveillance practices, nor economic incentives to file an action or complain to regulatory agencies, especially when there is no material or financial harm, so they *habituate* to such surveillance practices. On the other hand, it took some time between the first FTC action towards Facebook and the first denounces of privacy invasion. When the FTC announced the first settlement, Facebook seems to be very conscious about the necessity to modify its practices and present a set of *adaptations* to make users more comfortable while spending their time in the social network. Nevertheless, the first FTC action in 2012 was not compelling enough to dissuade Facebook from its practices of sharing and transferring behavioral data carelessly. On the contrary, in the period between the two FTC actions, Facebook, through *redirection* configurations, even improved its practices, having been very successful in concealing them until then.

The systematic privacy wrongdoings undertaken by Facebook in recent years, culminating with the Cambridge Analytica investigation, led ex-FTC Commissioner David

[452] ZUBOFF, op. cit., p. 95.
[453] Ibid at 96.
[454] Id.

Vladeck to argue that Facebook's actions were "*calculated and deliberate, integral to the company's business model, and at odds with the company's claims about privacy and its corporate values*".[455] Therefore, it brings the question of whether Facebook will adopt consistently the provisions depicted in the 2019 Order. Commissioners Rebecca Slaughter and Commissioner Rohit Chopra were skeptical in their dissenting statements on the matter and voted for litigating against Facebook before the Judiciary, rather than settle, despite the risks involving going to court. The dissenters considered that this second settlement was too premature and, consequently, the FTC lost the opportunity to dive deeper into Facebook's business model and its profit-making. They converged on three main points.

Firstly, although the $5 billion penalties is an enormous and unprecedented amount, Facebook's gross annual revenue increased from five billion to over fifty billion dollars in the period between the issue of the first FTC investigation in 2012 and the second one, initiated in 2018.[456] Such a fine, comparing to the amount Facebook has earned over six years and the impact the injury caused on public and democratic institutions, may not have the desired effect of forfeit undue gains and deter the company from engaging again in privacy violations. Facebook conduct not only violated the previous order issued by the Commission but also permitted reckless sharing of massive amounts of data, occasioning the creation of detailed profiles to be used for manipulation of voters.[457] Although this is the most expressive penalty applied by the Agency, it resembles *the Google* case in the sense that the gains derived from the violation of the order surpass the penalty applied, especially considering the substantial increase of Facebook's profits through the years. Secondly, the second settlement released Facebook executives, particularly Mark Zuckerberg, from any kind of civil liabilities under Section 5 for their conduct while driving the company's business, whereas in the past the FTC target executives and officers of small businesses.[458] Thirdly, the two dissenting statements are skeptical about the effectiveness of mechanisms and orders imposed on Facebook, as the 2019 Order did not provide any restriction on Facebook's collection, sharing, or use of personal data, leaving to the company the task to demand users' consent and classify what would constitute a

[455] VLADECK, David C. Facebook, Cambridge Analytica, and the Regulator's Dilemma: Clueless or Venal?, **Harvard Law Review Blog**. [Cambridge], Apr. 4, 2018. Available at https://blog.harvardlawreview.org/facebook-cambridge-analytica-and-the-regulators-dilemma-clueless-or-venal/.
[456] Federal Trade Commission, Dissenting Statement of Commissioner Rebecca Kelly Slaughter at 8, *In re Facebook, Inc.*, File No. 182 3109 (Jul. 24, 2019) and Federal Trade Commission, Dissenting Statement of Commissioner Rohit Chopra at 16, *In re Facebook, Inc.*, File No. 182 3109 (Jul. 24, 2019)
[457] Federal Trade Commission, Dissenting Statement of Commissioner Rebecca Kelly Slaughter at 9.
[458] Federal Trade Commission, Dissenting Statement of Commissioner Rebecca Kelly Slaughter at 14, *In re Facebook, Inc.*, File No. 182 3109 (Jul. 24, 2019) and Federal Trade Commission, Dissenting Statement of Commissioner Rohit Chopra at 19-20, *In re Facebook, Inc.*, File No. 182 3109 (Jul. 24, 2019).

permissible purpose to third-party access consumer's data. Besides, the settlement left Facebook broadly immune to unaddressed violations. Both dissenters were vocal in diagnosing Facebook's repeated conduct as inherent in its surveillance-based business model.

The critics brought in the dissent statements explicit the difficulty found by regulatory bodies in regulating private surveillance. Indeed, one must recognize that governmental authorities are still in a grey area, adapting and learning more about this new mode of capitalist production, in which regulatory goals involve not only address potential harms to consumers' health and security, but also social and political harms that are more subtle. Notwithstanding, considering all the concerns and explanations explored in this work, there are two axes on which public authorities must focus. First, improve the FTC monitoring capability, because effective regulation, relying or not on robust rulemaking, depends heavily on the monitoring capacity of public agents. Second, reformulate the privacy regulation paradigm based on control over information in order to give an account for a privacy model in which its collective dimension is taken into consideration. The FTC privacy regulation has majorly consisted of providing guidance to industries and interfered through enforcement action when it concludes that a company does not follow the Commission's understandings. Although the FTC Act grants extensive authority for monitoring of business, that is, for routine collection of nonpublic information of targeted companies, the FTC has not heavily relied on this regulatory resource and has maintained its focus on enforcement action.[459] Van Loo explains that the policy choice between monitoring and ex-post enforcement reflects a regulatory tradeoff between "police patrols" and "fire alarms" as "*policy designers can devote resources to search routinely for problems—as police do when patrolling the streets—or can wait for someone to pull a fire alarm to alert the authorities*".[460] Thus, the potential advantage of regulatory monitoring consists of its focus on preventing harm rather than remedy it or punish it. Besides, the routine and systematic collection of nonpublic information about the targeted industry is essential for regulators' understanding of an economic sector, identification of potential threats, and formulation of policies. Against the adoption of a monitoring mechanism, one might argue that the FTC adopted such tools in consent decrees but it had not prevented companies such as Google and Facebook from recidivism. As seen, when the FTC settles with the company, it

[459] VAN LOO, The missing regulatory state: monitoring businesses in an age of surveillance, p. 1571. ("the FTC's authorizing statute, when viewed in the context of judicial precedent and the normative foundations for monitoring, indicates that the FTC could—without any congressional action—monitor businesses far more extensively than it traditionally has").
[460] Van Loo, p. 1578.

usually adopts *post factum* monitoring mechanisms to verify if the enterprises are complying with the terms of the consent order for long periods, twenty years, a considerable period.

Improvement of the Commission's capacity to monitor platforms directly implies budgetary and personnel resources improvements. The FTC has a dual mandate to protect competition and consumers in a significant part of American industry. The Bureau of Consumer Protection, particularly the DPIP, is responsible for, among other subjects, privacy and security matters. Comparing those numbers with data protection authorities in European Union member states, for instance, FTC staff is considerably lean, especially when contrasted to the largest economies in the Old Continent:

Agency	Country	Staff members[1] (2019)	Population[2] (2019)	Staff / Population (per million)	GDP[2] (2019)	Budget[1] (2019)
Federal Trade Commission (FTC)	**United States**	**52 (DPIP) 612 (BCP)**	**328,239,523**	**0.15**	**US$87.73tri**	**US$171,19m (BCP)**
Commission nationale de l'informatique et des libertés (CNIL)	**France**	**215**	**67,055,854**	**3.2**	**US$2.71tri**	**€ 18,5m**
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)	**Germany**	**253**	**83,092,962**	**3.0**	**US$3.861tri**	**€25m**
Garante per la protezione dei dati personali (GPDP)	**Italy**	**170**	**60,302,093**	**2.8**	**US$2.0tri**	**€29,56m**
Agencia de Protección de Datos	**Spain**	**170**	**47,133,521**	**3.6**	**US$1.39tri**	**€15,19m**

Information Commissioner's Office (ICO)	**United Kingdom**	**680**	**66,836,327**	**10.1**	**US$2.82tri**	**€60,78m**

Table 1 Comparison between European data protection authorities in Europe and the FTC.

1. Staff and funding: Europe – Cullen International; FTC – Fiscal Year 2019 Congressional Budget Justification
2. Population and GDP: World Bank.

Although the BCP has a greater budget when compared to other data protection authorities in Europe, one must notice that the Bureau is also responsible for a wide variety of other subjects, such as advertising and credit, and finance. Besides, FTC staff devoted to privacy affairs is considerably scarce in contrast with other data protection agencies. However, it should be recognized that the massive collection of data and its improper uses have been in recent years a rising concern of the Commission. The creation of the Office of Technology Research and Investigation is a welcome measure in this sense.[461]Additionally, the FTC has made an effort to better understand the data broker industry in the United States – network companies that collect consumers' personal information and resell or share them with others - which, just as Facebook, has a tremendous capacity to collect, aggregate and transfer, mostly without consumers' awareness.[462] More recently, the FTC Commissioners expressed their concerns over social media and video streaming services for their capabilities to monitoring and monetizing comprehensive aspects of our personal lives, as the industry methods remains opaque, and decided to dive deeper through a Section 6(b) study[463] to assess their practices.[464] Those are important mechanisms to get a closer look at the data industry and have more consistent basis

[461] The FTC's Office of Technology Research and Investigation is housed on the BCP. The Office conducts studies, assess market practices and provide guidance to consumers and business concerning issues such as privacy, data security, connected cars, smart homes, and algorithmic transparency. It also assists FTC enforcers providing technical expertise, investigative assistance, and training. FEDERAL TRADE COMMISSION, Office of Technology Research and Investigation, available at https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/office-technology-research-investigation (last access Jun 1, 2021).
[462] For further information about data brokers, *see* FEDERAL TRADE COMMISSION, **Data brokers: a call for transparency and accountability**, Washington, D.C., 2014.
[463] Section 6(b) of the FTCA empowers the Commission to demand information about the entity's "organization, business, conduct, practices, management, and relation to other corporations, partnerships, and individuals."
[464] FEDERAL TRADE COMMISSION, Joint statement of FTC commissioners Chopra, Slaughter, and Wilson regarding social media and video streaming service providers' privacy practices, File No. P205402 (December 14, 2020) https://www.ftc.gov/public-statements/2020/12/joint-statement-ftc-commissioners-chopra-slaughter-wilson-regarding-social ("The FTC wants to know how many users these companies have, how active the users are, what the companies know about them, how they got that information, and what steps the companies take to continue to engage users. The inquiry also asks how social media and video streaming companies process the data they collect and what kinds of inferences they can make about user attributes, interests, and interactions. The FTC wants to understand how business models influence what Americans hear and see, with whom they talk, and what information they share. The questions push to uncover how children and families are targeted and categorized. These questions also address whether we are being subjected to social engineering experiments. And the FTC wants to better understand the financial incentives of social media and video streaming services").

to initiate an enforcement action. Maybe an enhancement of FTC's monitoring would mitigate the effects of the dispossession cycle depicted by Zuboff.

On the other hand, the Facebook case demonstrates the structural difficulties of the privacy approach based on control over information, and its limits to address privacy harms derived from big data and predictive analysis. Facebook users do not have doubts that the social network collects a vast quantity of personal information, but are little aware of the predictive capacity about their political preferences in a wide array of subjects, just as the pregnant teenager who bought supplies at Target but had never revealed her condition to the retail store. The prohibition to misrepresent data privacy and security standards in the majority statement in the Facebook case still does not seem to address these concerns. However, an approach that recognizes privacy as a dimension of citizenship is capable of hold users accountable for who needs data, for what purposes, and how configurations shape our perceptions.[465] A possible alternative to reach a more democratic dimension of privacy is the establishment of a due process clause to address predictive privacy harms.[466] More than granting individuals notice about the data uses and processes that employ predictive analysis, the recognizance of a data due process right should provide an opportunity to access the audit trail in the predictive process and intervene in it.[467] The existence of a data due process allows understanding the path of platforms choices to provide or not certain kinds of information is an important mechanism to turn information technologies more transparent, mitigating the "black-box effect", and held them more accountable. As an information privacy authority, the FTC would have an important role in monitoring and auditing those processes.

3.2.3 The third complaint against Facebook: “it is better buy than compete”

One year after the FTC application of the $5 billion fine to Facebook, in December 2020, the Commission took another step against the social network and filed a complaint before the Federal District Court for the District of Columbia, charging the Facebook group for holding of monopoly power in the market for personal social networking under Section 2 of the Sherman Act and Section 5 of the FTC Act. In a 3-2 decision, the Commission considered that, in the last ten years, Facebook, the dominant social network in the United States since 2011,

[465] MOROZOV, Evgeny. Facebook invades your personality, not your privacy. **Financial Times**. [s.l.]Aug. 10 2014. Available at https://www.ft.com/content/dd5e5514-198d-11e4-8730-00144feabdc0. Last access May 25, 2021.
[466] CRAWFORD, Kate; SCHULTZ, Jason, Big data and due process: toward a framework to redress predictive privacy harms, **Boston College Law Review**, v. 55, n. 13, p. 93–128, p. 124, 2013.
[467] Id.

has maintained its monopoly position through the acquisition of potential competitors, Instagram and WhatsApp, and the imposition of unjustifiable restrictions to third-party apps, preventing the emergence of new competitors.[468] Currently, the case is pending in the district court.

Corporate acquisitions are indeed common in high-tech industries, and not all operations imply an antitrust violation. An incumbent firm may buy a startup not because the latter is seen as a direct competitor, but because the products or services developed can function as inputs or complements to the incumbent's business.[469] On the other hand, acquisitions can also lead to verticalization, with incumbent firms entering new markets and expanding their domains. In fact, it can be challenging to assess whether a blossoming startup has the potential to grow and compete effectively with a dominant firm. However, independently of the outcomes, the entrance of newcomers in markets is always beneficial for consumer welfare, as they attempt to bring innovation and quality to compete with established firms.[470]

The investigation carried out by the FTC demonstrates that Facebook's decision to buy both Instagram and WhatsApp had roots in the fear these two companies would surpass Zuckerberg's company in the social network market. Social networks have become extremely popular in the United States and part of the adult population's everyday life. In February 2021, approximately 72% of adults in the U.S use at least one social network, being 69% of them Facebook users, 40% Instagram users, and 23% WhatsApp users.[471] Besides, with regard to frequency, 70% of Facebook users and 59% of Instagram users access the social network daily.[472] The emergence of Instagram, a mobile app that allows users to take, edit, share, and comment on their photos, raised concerns among Facebook staff because of its templates and functionalities that made it more comfortable to be used through mobile apps when compared with Facebook, a social network designed to be used in desktops. [473] Instagram was developed in a time of technological transition when Internet users were migrating from desktops to

[468] FEDERAL TRADE COMMISSION. FTC sues Facebook for illegal monopolization (Dec. 9, 2020), https://www.ftc.gov/news-events/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization; FEDERAL TRADE COMMISSION. **Federal Trade Commission v. Facebook Inc.,** Case 1:20-cv-03590-JEB, US District Court for the District Court of Columbia, Dec. 9, 2020 (Complaint for injunctive and other equitable relief). Available at https://www.ftc.gov/enforcement/cases-proceedings/191-0134/facebook-inc-ftc-v.

[469] BRYAN, Kevin A; HOVENKAMP, Erik, Antitrust Limits on Startup Acquisitions, **Review of Industrial Organization**, v. 56, n. 4, p. 615–636, p. 616, 2020.

[470] MORTON, Fiona M Scott; DINIELLI, David C, **Roadmap for an Antitrust Case Against Facebook**, Omidyar Network, June 2020, p. 21.

[471] SOCIAL Media Fact Sheet, Pew Research Center. [s.l.] Apr. 7, 2021. https://www.pewresearch.org/internet/fact-sheet/social-media/#how-often-americans-use-social-media-sites.

[472] Id.

[473] FEDERAL TRADE COMMISSION. **Federal Trade Commission v. Facebook Inc.,** Case No. 1:20-cv-03590-JEB (Complaint for injunctive and other equitable relief, p. 23).

smartphones, devices that combined high-quality cameras and Internet access and starting to use social networks through smartphone apps. In the meantime, Facebook employees were also investing in its mobile app and photo-sharing features, but Mark Zuckerberg concluded it would be inviable to compete on an equal basis with Instagram.[474] Fearing the emerging app, Facebook took the decision to buy it and publicized the decision on April 9, 2012.

Zuckerberg was not relieved, though. With the popularization of smartphones, people were rapidly leaving SMS message services and transitioning to over-the-top mobile message apps. Facebook feared that a messaging app would enter the social networking market, either by launching new functionalities to the app or a new social network and rise as a strong competitor.[475] By that time, it was WhatsApp, an emerging and worldwide popular app, which seemed to constitute that potential threat. Facebook workers feared that, with improvements, WhatsApp would migrate from a single messaging app to a social network market with a sustained database of users. Thus, in 2014, Facebook acquired WhatsApp for $19 billion, its most expensive acquisition. Despite the record-breaking value, until recently Facebook endured difficulties to monetize it, which would suggest that its goal was to exclude an eventual rival from the market.[476] According to the FTC, the acquisition of both Instagram and WhatsApp raise suspect of monopolization strategy given the overpayment for both firms, much higher than their market valuation. In fact, since its creation, Facebook group has acquired nearly 100 companies[477], some of them to enhance its products and offer compliments to its platforms, such as Giphy, a mix of database and search engine through which users may find and share short looping videos.

The FTC also considered that Facebook undermined the growth of third-party apps interoperating with the social network. Third-party apps have access to Facebook's data through Facebook's application programming interfaces ("APIs"), such as the "Find Friend" API, which allowed Facebook users to find friends while using third-party apps and to invite them. However, to grant this access, Facebook has imposed a series of conditions that deterred them from developing similar core functions of Facebook that might compete with it, as well as from

[474] Ibid., p. 27.
[475] Ibid., p. 30.
[476] MORTON, Fiona M Scott; DINIELLI, David C, **Roadmap for an Antitrust Case Against Facebook**, Omidyar Network, June 2020, p. 21.
[477] For a complete list of Facebook, acquisitions *see* LIST of mergers and acquisitions by Facebook, **Wikipedia: the free encyclopedia**. Available at https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Facebook. Access on May 18, 2021.

connecting in many ways to other social networks.[478] Third-party apps were forbidden to export data to competitors' social networks or to any app that mimics core functions of Facebook services. If the apps violated these policies, Facebook would finish their access to APIs.[479] Moreover, Facebook has used a software named Onavo to monitor how often users accessed third-party apps and, based on the information received, make decisions to either acquire high-performing companies, such as Instagram, or hinder them by denying or blocking access to Facebook's APIs.[480] This occurred to Vine, a video-sharing platform. Vine users could find their Facebook friends through "Find Contacts" API but Facebook decided to block the feature. APIs such "Find Contacts" allow interoperability between platforms and mitigation of strong network effects characteristic of the social network market.[481] These constraints, in the Commission's understanding, refrained promising third-party apps from developing new functionalities and compete with Facebook.

The Commission concluded that those conducts lead Facebook to maintain a monopoly position on unfair terms through practices to deter, suppress and neutralize competition in the social network's market. The FTC complaint against Facebook does not directly address the discussion about whether the concentration of datasets is an antitrust problem. According to the Commission's complaint, Facebook's greater concern over Instagram and WhatsApp relied upon their potential to become strong competitors to Facebook. However, in a certain way, through the acquisition of Instagram and WhatsApp, Facebook substantially enlarged its datasets. With more individuals using Facebook's services, new and smaller companies endure to compete in equal terms. Opponents of broad antitrust approach in Big Data matters have argued that data markets, such as social networks markets, are pro-competitive, with low barriers to entry, as data collection is cheap, non-rivalrous, simply requiring an insight into users' needs, independently of any network effect.[482] Besides, the collection of data alone is not enough, being necessary for a company to have the means to process data, what requires other variants, such as qualified staff, speed to innovate, quality of service, and attention to users need.[483] However, this argument has limitations. As seen previously, data-driven markets face barriers to entry due to network effects, which are substantially strong in the social network

[478] Federal Trade Commission v. Facebook, Inc., Case No. 1:20-cv-03590, Complaint for injunctive and other equitable relief, p. 41.
[479] Id.
[480] Ibid. at 22.
[481] Ibid. at 46.
[482] SOKOL; COMERFORD, Antitrust and regulating big data, p. 1136.
[483] Ibid. p. 1138-1139.

market. As consequence, users tend to endure high switching costs. [484] Data will only be freely available and easy to collect if one of the sides of the market is populated, meaning that there must be persons or companies using the service provided for data to be harvested. Thus, even the most prominent engineering team must have access to a reasonable amount of data to improve the services provided. Data fuels the work of complex algorithms and statistical analysis, which will disclosure patterns of behavior, indicate trends, and lead to more guaranteed and profitable results. Indeed, as argued by Maurice Strucke and Allen Grunes, "if personal data were as freely available as sunshine, companies would not spend a considerable amount of money offering free services to acquire and analyze data to maintain a data-related competitive advantage".[485]

Besides, even if someone managed to bring an outstanding alternative, big techs have the means to deter their users to see something. The importance of access to Facebook data through APIs illustrates well this problem. Facebook used its control over its infrastructure to constrain activities third-party apps that interoperate through APIs, determining that data could only be used on the condition that those apps do not compete with Facebook and Messenger and deliberately blocking apps that would raise as their potential rivals, such as Vine. In this sense, probably it is not without reason that Facebook's fiercest rival is ByteDance's TikTok, a Chinese app that allows users to create, edit and share short videos. TikTok grew at first in China, where Facebook services are not allowed to penetrate, and achieved Western countries after its consolidation in the Chinese market. The FTC considered that the limitations undertaken by Facebook suppressed incentives to apps innovate and provide better quality products to users and helped Facebook sustain a monopoly position in the social network market through exclusionary practices, which configure unfair methods of competition under Section 5 of the FTC Act.

One might question whether is incoherent the FTC accuses Facebook of violation of antitrust law with regards to the limitation on access to data to third-party apps while in the previous year the Commission fined $5 billion Facebook precisely due to excessive data sharing

[484] **Federal Trade Commission v. Facebook, Inc**., Case No. 1:20-cv-03590, Complaint for injunctive and other equitable relief, at p. 3. ("In particular, because a personal social network is generally more valuable to a user when more of that user's friends and family are already members, a new entrant faces significant difficulties in attracting a sufficient user base to compete with Facebook. Facebook's internal documents confirm that it is very difficult to win users with a social networking product built around a particular social "mechanic" (i.e., a particular way to connect and interact with others, such as photo-sharing) that is already being used by an incumbent with dominant scale. Even an entrant with a "better" product often cannot succeed against the overwhelming network effects enjoyed by a dominant personal social network").
[485] STUCKE; GRUNES, op. cit., p. 7.

with the same third-party apps. In fact, there is no incoherence in this case for two reasons. First, Facebook limited access to data not based on privacy practices but with the intent to curb the development of any services that would menace its dominant position. Second, sharing data through APIs is a form of interoperability, which, as seen in chapter one, is not necessarily harmful to consumers if respected privacy design and rules. Interoperability indeed may be an important measure to limit network effects and foster competition in data-driven markets. In addition, a good interoperable design allows users to have better control over their data. Therefore, maybe in that case, in order to address the concerns related to privacy, the FTC should create a more robust regulation on interoperability operations, with the possibility to held third parties liable.

In its concluding remarks, the FTC claimed that, through the conducts depicted above, Facebook has deprived both users and advertisers of the benefits of competition. According to the Commission, users benefit include additional innovation; quality improvements; and consumer choice, including privacy protection options regarding but not limited to data collection and usage.[486] On the other hand, advertisers would benefit from additional users to advertise to; lower advertising prices; more innovation; quality enhancements; and choice over the social network that better suits their preferences.[487] As Facebook's products are offered for free and in unlimited quantities, the FTC seemed to consider in its monopoly power analysis that there is a loss of quality of the services provided in the market due to Facebook conducts, although not being explicit about its relationship to the concentration of datasets in the company. Besides, the Commission expressly affirmed that Facebook practices lessened consumer choices over privacy practices in the market. As seen previously, in multi-sided markets where a service is offered free, privacy protections may be a form to attract consumers and become a non-price dimension of competition.[488] In fact, Facebook group dominance of expressive market power in social networks prevented users' presume mechanisms such "Delete Facebook" campaign in response to the Cambridge Analytica scandal from going ahead.[489] "Delete Facebook" but where to go, then? Despite the legitimate privacy concerns, it was unlikely that an expressive amount of users would just leave behind the network of contacts

[486] FEDERAL TRADE COMMISSION. Facebook, Inc., Case No. 1:20-cv-03590, Complaint for injunctive and other equitable relief, at p. 49.
[487] Ibid.
[488] OKULIAR; OHLHAUSEN, op. cit., p. 100; STUCKE; GRUNES, op. cit.
[489] A quarter of Facebook users in the United States reported have deleted their accounts and near a half have adjusted their privacy settings, *see* PERRIN, Andrew, Americans are changing their relationship with Facebook, Pew Research Center (Sep. 5, 2018), https://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/.

built in there and reshape how they interact with family members and friends.[490] It is unlikely that there is a turning back. Similarly, in January 2021, WhatsApp gave its Brazilian users notice regarding changes in its Privacy Policies related to data sharing with Facebook regarding purchases through WhatsApp Business service.[491] WhatsApp warned those who did not agree with the new terms would have their apps blocked until he or she accepts it. The problem lies in the fact that approximately 90% of mobile users in Brazil use WhatsApp, so be disconnected from this network would imply be excluded from a vast list of contacts, as many of them do not use alternative chat apps, such as Telegram or Signal. Sometimes be excluded from such a network is simply not viable. However, due to the bad repercussion of the policy changes, leveraged by protests of non-governmental organizations and a considerable amount of users, the Brazilian Data Protection Authority determined that WhatsApp must postpone the adherence to its new Privacy Policy to verify whether it complies with Brazil' General Data Protection Law.[492]

The position adopted by the FTC in the Facebook complaint seems to be a change in comparison with its previous understanding in Google/DoubleClick merger decision, where it considered that privacy and other non-price aspects should not be encompassed by the antitrust analysis. As seen in chapter two of this work, the influence of the Chicago School claimed that the goal of antitrust was to promote consumer welfare and led consumer price to the center of anticompetitive conducts assessment, rather than practices that could curb competition on a given market. Consequently, an operation that promotes economic efficiency would be acceptable even if it resulted in higher concentrated markets, so practices such as vertical integration and predatory pricing moved away from courts' oversight.[493] Tim Wu considers that courts and academics, while embraced this narrow reading of the Sherman Act, have left behind the fundamental and historical goal of antitrust, which is to check on political and economic power of monopolies.[494] The consumer welfare standard, though, after decades, has not brought

[490] *See* e.g. GYUNN, Jessica, Delete Facebook? It is a lot more complicated than that, USA Today (Mar 28, 2018), https://www.usatoday.com/story/tech/news/2018/03/28/people-really-deleting-their-facebook-accounts-its-complicated/464109002/.
[491] WHATSAPP avisa que irá compartilhar dados dos usuários com o Facebook. **G1.** [s.l.] Jan. 6, 2021. Available at https://g1.globo.com/economia/tecnologia/noticia/2021/01/06/whatsapp-comeca-a-avisar-que-ira-compartilhar-dados-dos-usuarios-com-o-facebook.ghtml. Last access on May 30, 2021.
[492] WHATSAPP inicia nova política de privacidade neste sábado; veja o que muda. **G1.** [s.l.] May 15, 2021. Available at https://g1.globo.com/economia/tecnologia/noticia/2021/05/15/whatsapp-inicia-nova-politica-de-privacidade-neste-sabado-veja-o-que-muda.ghtml.
[493] KHAN, Lina M. Amazon – An Infrastructure Service and Its Challenge to Current Antitrust Law *In* MOORE, Martin; TAMBINI, Damian. **Digital Dominance: the power of Google, Amazon, Facebook, and Apple**. New York, Oxford University Press, 2018.
[494] WU, op. cit., 2018, p. 88.

scientific certainty because it is indeed really difficult in practice to assess the effects of such highly complex transactions.[495] Therefore, courts should verify whether conduct is capable of suppressing or destroy competition. Considering the arguments brought by the FTC in Facebook's complaint, it seems that the Commission is carrying on a claim that relies on non-price elements to demonstrate Facebook's anticompetitive conduct, which means that it could be mitigating the Chicago School method on multi-sided digital markets. It is worth notice, however, that the FTC decision to file this antitrust claim was far from being unanimous, which might indicate that antitrust action against platforms is not a matured issue even inside the Commission. Nonetheless, the submission of such a case to the courts is important to the debate about antitrust regulation of platforms and digital markets as a whole.

3.3- Conclusions of the chapter

As seen in the previous chapters, in platforms' business model the existence of surveillance apparatus to gather data along with the ownership of the means is essential for the constitution of platforms' gatekeeping capacity. Therefore, an effective regulatory policy to limit platform surveillance and gatekeeping should reflect a coordinated effort in both realms. The FTC has a broad mandate to both protect consumer rights and promote competition through a wide range of economic sectors, which gave the agency a privileged view to formulate regulatory policies concerning the data-based industry. Despite the existence of limitations in the Commission's authority in both realms, and the necessity to perfect its regulatory toolkit, in recent years there has been an increasing concern about the potential harms derived from platform markets.

The three complaints filed against Facebook are symptomatic of the attention given to this theme. In particular, at the time of the second complaint, which led the FTC to reopen the privacy case against Facebook, the Agency was under intense political and social scrutiny due to the Cambridge Analytica revelations. After all, years before, Facebook settled with the FTC and the consent order was still in effect when the scandal broke out, but the Commission had not yet identified any failure to comply with Facebook's obligations. The potential harm to the democratic process in the United States raised a fire alarm in many governmental instances, the FTC included, what led the Commission to apply the largest fine in its history until then. It was necessary to give a proper response to American society. However, it appears that the Commission considered that reliance only on consumer privacy enforcement probably would

[495] Ibid., p. 135.

not be enough to restrain Facebook's power over the network. So, it filed one year later an antitrust complaint against the company for its aggressive anti-competitive practices with the potential to break up the Californian technology conglomerate. The case probably will drag on for years in courts. Perhaps in the end Facebook's companies will not be torn apart, but similarly to the Microsoft case, it can drain substantial corporate efforts that otherwise would be directed to other fronts – and ironically gave room to the emergence of Google, Facebook, and Amazon. Maybe this can be an opportunity for a new generation of businesses to emerge. And so the wheel turns.

CONCLUSION

Online platforms have become important points in the networks that intermediate information flows, but simultaneously create new forms of competition and control. Whereas platforms can bring individuals and groups together, they also take advantage of massive data collection and generate more value.[496] The dominance of few technology conglomerates, GAFAM in particular, who function as gatekeepers, raise concerns about their influence over the dissemination of ideas and political discourse, particularly due to their capability to find patterns of behavior and nudge users. Probably political harms, such as those inflicted by Cambridge Analytica, are among the most feared surrounding platforms.[497] In this sense, government authorities have realized that the power over networks of informational capitalism model industry, the platform, configured a problem that should be regulated. Although the FTC in the last ten years has increased its oversight over these companies, the cases against Facebook represented a turning point in its regulatory policy towards the platform industry. As David Vladeck observes, the FTC has limited statutory authorization and cannot investigate the data processing proceedings to shape users' political views undertaken by Cambridge Analytica.[498] However, through its consumer privacy authority, it attempted to address Facebook's misuse of data imposing not only because of the billionaire value of its fine but also due to the new array of privacy obligations the Commission subjected the Mark Zuckerberg's company. Probably the antitrust action against the company one year later also is, in some way, a reflection of the Commissions' attempt to mitigate Facebook's power through a second front.

Currently, due to its dual mandate, the FTC has a singular capacity to build regulatory policy on both fronts, consumer privacy, and competition, and is embedded of broad powers to conduct investigations and enforcement procedures. However, it does not mean that its enforcement policy has limitations or areas of improvement. In the information privacy realm, although the Commission has adopted an enforcement-based regulation in deprivation of rulemaking, and has thickened its understandings through the years, its capacity to open investigations is still restricted. Until May 2021, the FTC filed 278 complaints in privacy and security matters, despite the number of enforcement actions per year have increased over time, although still very limited when considered the amount of data-related business in the United

[496] SRNICEK, op. cit, p. 94.
[497] FUKUYAMA *et al*, op. cit.
[498] VLADECK, op. cit.

States.[499] A most effective regulatory policy would pass necessarily to an increase in its personnel. In fact, the current FTC regulatory action in online privacy matters seems to have focused only on the most hideous cases. In addition, it would be important for the FTC to develop its monitoring activities, rather than focus majorly on repressive action. This measure is especially important for the development of more effective regulation because until the end of an investigation it can have passed much time from the moment of the privacy harm. Thus, strengthen the Commission's monitoring capability would be essential to act preventively. Another limitation of the FTC concerns its emphasis on consumer choice over information, which could be reframed through the recognition of privacy as a means to exert citizenship and, as consequence, a due process right in data collection and processing, mitigating the "black-box effect".

In the antitrust realm, the case against Facebook shows that the Commission decided to combat conducts undertaken by platforms through its competition authority, which indicates a change of orientation, although the decision to file the complaint was not unanimous. The FTC seems to be into a trend also observed in other governmental authorities on filing lawsuits against Big-Techs, considering that the DOJ along with states filed a lawsuit against Google in October 2020 for abuse of its monopoly position on search engine market and District of Columbia lawsuit against Amazon in May 2021. The million dollars question is whether courts will uphold the arguments brought by regulators, as common law has long been under influence of Chicago School's principles. The tendency, though, is that these lawsuits will drag on for years, so a final answer will not come for a while.

There have been some proposals towards the creation of sectoral regulation or even of a new digital regulator, to address the risks and potential harms that may occur in digital markets, but there is nothing concrete pointing in one of these directions.[500] As Hoofnagle, Hartzog, and Solove remark, since its foundation in the Commission has adapted to new technologies, passing through newspaper, radio, television, and Internet fraud, so it can deal with new data-driven business models.[501] While there is no decision from US Congress, the FTC could use its guidance authority to design more objective criteria for assessment of the quality of a product or service offered for free; develop better and more transparent

[499] FEDERAL TRADE COMMISSION. **Cases and Proceedings: Advanced Search**. Available at https://bit.ly/3cFZsLP. Last access on May 30, 2021.
[500] ZINGALES, Luigi; ROLNIK, Guy; LANCIER, Filippo Maria. op. cit., p. 100-101; 104.
[501] HOOFNAGLE, Chris Jay; HARTZOG, Woodrow; SOLOVE, Daniel J., The FTC can rise to the privacy challenge, but not without help from Congress. **Brookings.** [s.l.], Aug. 8, 2019. Available at: <https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/> Last access on June 10, 2021.

requirements to assess mergers and acquisitions review; and explain the criteria to assess consumer welfare in two or multi-sided markets. Another important measure that would mitigate network effects and switching costs consist in the imposition of interoperability requirements, just as occurred in the past with telecommunications networks. Just as AT&T has the obligation to connect its users to T-Mobile's ones, users of social media would be able to interconnect. Taking off the power of gatekeepers to impose barriers to traffic over different networks would empower consumer choice.

This work aimed to shine a light on the recent efforts undertaken by the FTC to regulate some of the potential risks derived from platforms' practices and remedy inflicted harms, particularly through the analysis of the three complaints against Facebook. It is a small contribution towards a better understanding of how regulatory authorities around the globe have been reacting to platforms' increased influence. As a suggestion, further works in this field could also cover how competition and consumer privacy policies of regulatory authorities in other countries are intertwined, or the relationship between surveillance apparatus and its reflections on freedom of speech over the networks.

REFERENCES

ACQUISTI, Alessandro; GROSSKLAGS, Jens, What can behavioral economics teach us about privacy?, **Digital Privacy: Theory, Technologies, and Practices**, p. 363–377, 2007.

AMPUJA, Marko; KOIVISTO, Juha. From 'Post-Industrial' to 'Network Society' and Beyond: The Political Conjunctures and Current Crisis of Information Society Theory, **TripleC: Communication, Capitalism & Critique**, v. 12, n. 2, p. 447–463, 2014.

ANDREJEVIC, Mark. The big data divide. **International Journal of Communication,** v. 8, 1673–1689, 2014.

_____. Automating Surveillance, Surveillance & Society, v. 17, p. 7–13, 2019.

ANON, Dennin, How cookies track you around the web and how to stop them. **Priavacy.net,** [s.l.] Feb. 24,2018. Available at <https://privacy.net/stop-cookies-tracking/>. Last access Oct. 2, 2020.

AUXILIER, Brooke et al. Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. **Pew Research Center**, [s.l.] Nov. 15 2019. Available at https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/. Last access on Oc. 2, 2020.

BALKIN, Jack M., Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society, **New York University Law Review**, v. 79, n. 1, p. 1–55, 2004.

_____. The Constitution in the National Surveillance State. **Minnesota Law Review**, v. 93, n. 1, p. 1–25, 2009.

BARLOW, John Perry. **Selling Wine Without Bottles : The Economy of Mind on the Global Net**. Electronic Frontier Foundation. [s.l.], 1994. Available at: https://www.eff.org/pages/selling-wine-without-bottles-economy-mind-global-net. Last access Jun 17, 2020.

_____. A Declaration of the Independence of Cyberspace. **Electronic Frontier FoundationElectronic Frontier Foundation**, 1996. Available at: <https://www.eff.org/cyberspace-independence>. Last access Jun. 17, 2020.

BARWISE, Patrick; WATKINS, Leo. The evolution of digital dominance: how and why we got to GAFA. In: MOORE, Martin; TAMBINI, Damian (Orgs.), **Digital Dominance: the power of Google, Amazon, Facebook, and Apple**, New York: Oxford University Press, 2018.

BAUMER, David L.; EARP, Julia B.; POINTDEXTER, J. C. Internet privacy law: a comparison between the United States and the European Union. **Computers & Security**, p. 400–412, 2004.

BELL, Daniel. The coming of the post-industrial society, **Educational Forum,** v. 40, n. 4, p. 575–579, 1976.

BENKLER, Yochai, From Consumers to Users : Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access, **Federal Communications Law Journal**, v. 52, n. 3, p. 561–579, 2000.

BIGNAMI, Francesca. Scherms II: the right to privacy and the new illiberalism. **Verfassungsblog**, Jul 29, 2020. Available at https://verfassungsblog.de/schrems-ii-the-right-to-privacy-and-the-new-illiberalism/. Last access Nov. 20, 2020.

BLACKMAN, Colin R. Convergence between telecommunications and other media How should regulation adapt? **Telecommunications Policy**, v. 22, n. 3, p. 163–170, 1998.

BORK, Robert. **The antitrust paradox:** a policy at war with itself. New York: Free Press, 1993.

BOYLE, James. A Theory of Law and Information: copyright, spleens, blackmail, and insider trading. California Law Review, v. 80, n. 6, p. 1413–1540, 1992.

____. Foucault in cyberspace: surveillance, sovereignty, and hardwire censor, **University of Cincinnati Law Review**, v. 66, p. 177–205, 1997.

_____. The second enclosure movement and the construction of the public domain. **Law and Contemporary Problems**, v. 66, n. 33, p. 33–74, 2003.

BROWN, Wendy. **Neo-liberalism and the end of liberal democracy. Theory and Event, v. 7, n. 1, 2003.** Available at https://muse.jhu.edu/article/48659. Last access on Aug. 23, 2020.

BRYAN, Kevin A; HOVENKAMP, Erik, Antitrust Limits on Startup Acquisitions, **Review of Industrial Organization**, v. 56, n. 4, p. 615–636, p. 616, 2020

CADWALLADR, Carole; CAMPBELL, Duncan. Revealed: Facebook's global lobbying against data privacy laws. The Guardian, [s.l.] Mar. 2 2019, Available at https://www.theguardian.com/technology/2019/mar/02/facebook-global-lobbying-campaign-against-data-privacy-laws-investment. Access on Aug. 18, 2020.

CARLSON, Nicholas. Here's the biggest threat to Facebook, and what Facebook is doing about it. **Business Insider**, Feb. 6, 2012. Available at https://www.businessinsider.com/heres-the-biggest-threat-to-facebook-and-what-facebook-is-doing-about-it-2012-2.

CASTELLS, Manuel. **Communication Power**, 1 ed., New York: Oxford University Press, 2009.

_____. **The Information Age, vol. 1: The Rise of the Network Society**, 2 ed. Oxford: Blackwell Publishing, 2010.

CHANDER, Anupam. How law made Silicon Valley, **Emory Law Journal**, v. 63, n. 639, p. 639–694, 2014.

CLARKE, Roger A, Information technology and dataveillance, **Communications of the ACM**, v. 37, n. 5, p. 498–512, 1988.

COHEN, Julie E. Configuring the networked citizen. In: SARAT, Austin; DOUGLAS, Lawrence; MERRILL UMPHREY, Martha (Orgs.), **Imagining New Legalities: Privacy and Its Possibilities in the 21st Century**, Stanford: Stanford University Press, 2012, p. 129–53.

_____. What privacy is for, **Harvard Law Review**, v. 126, n. 7, p. 1904–1933, 2013.

_____. **Between truth and power: the legal constructs of information capitalism**. New York: Oxford University Press, 2019.

COOPER, James C., Privacy and antitrust: underpants gnomes, the first amendment, and subjectivity, **George Mason Law Review**, v. 20, n. 4, p. 1129–1146, 2013.

CRAWFORD, Kate; SCHULTZ, Jason, Big data and due process: toward a ramework to redres predictive privacy harms, **Boston College Law Review**, v. 55, n. 13, p. 93–128, p. 124, 2013.

CUSTOS, Dominique. The rulemaking power of independent regulatory agencies. **American Journal of Comparative Law**, v. 54 (Supplement Issue), 615-640, 2006.

CYPHERS, Bennet; DOCTOROW, Cory. Privacy without monopoly: data protection and interoperability. **Electronic Frontier Foundation**, [s.l.] Feb. 12 2021. Available at: https://www.eff.org/wp/interoperability-and-privacy#Risksandmitigations. Last access Mar. 1, 2021.

DROESCH, Blake. Amazon dominates US commerce though its market share varies by category. **Emarketer**, [s.l.], April 27 2021. Available at https://www.emarketer.com/content/amazon-dominates-us-ecommerce-though-its-market-share-varies-by-category. Access on May 15, 2021.

ELECTRONIC PRIVACY INFORMATION CENTER. **Complaint and Request for Injunction, Google & DoubleClick, Inc.** [Washington], Apr. 20 2007, p. 2. Available at epic.org/privacy/ftc/google/epic_complaint.pdf.

EUROPEAN UNION. European Court of First Instance. Microsoft Corp. v. Commission, T-201/04, Sep. 17 2007. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62004TJ0201.

_____. Treaty Establishing the European Community art. 82, Nov. 10, 1997, 1997 O.J. (C340).

EZRACHI, Ariel; STUCKE. Maurice E., eDistortions: how data-opolies are dissipating the Internet's potential. **Promarket.** [s.l.], Mar. 27 2018. Available at https://promarket.org/2018/03/27/edistortions-data-opolies-dissipating-internets-potential/.

DUHIGG, Charles. How Companies Learn Your Secrets **The New York Times Magazine**, Feb. 16 2012.

FACEBOOK. **Annual Report 2020 (Form 10-K)**. [s.l.] Jan. 28 2021, p. 7. Available at https://investor.fb.com/financials/sec-filings-details/default.aspx?FilingId=14646367. Last access Mar. 20 2021.

_____. **Company Info**. [s.l.], [s.d.]. Available at https://about.facebook.com/company-info/ . Last access May 3 2021.

FEDERAL TRADE COMMISSION. **FTC Policy Statement on Unfairness.** Washington, Dec. 17, 1980. Available at https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness

_____. **Big Data:** a tool for inclusion or exclusion? Understanding the issues. [Washington]: [s.n.], Jan. 2016. Available at https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report.

_____.**Competition & Consumer Protection Authorities Worldwide**. Washington, D.C. Available at https://www.ftc.gov/policy/international/competition-consumer-protection-authorities-worldwide. Last access on Feb. 21, 2021.

_____. **FTC Policy Statement on Deception.** Washington, Oct. 14, 1983. Available at https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

_____. **Federal Trade Commission v. ReverseAuction.com, Inc**. Civil Action No. 000032, D.D.C. Available at https://www.ftc.gov/sites/default/files/documents/cases/2000/01/www.ftc_.gov-reversesl.htm.

_____. **Federal Trade Commission v. Vizio, Inc. and Vizio Inscape Services, LLC**. Case 2:17-cv-00758, US District Court for District of New Jersey, Feb. 3, 2017. (Complaint) Available at https://www.ftc.gov/enforcement/cases-proceedings/162-3024/vizio-inc-vizio-inscape-services-llc.

_____. **Federal Trade Commission v. Facebook Inc.**, Case 1:20-cv-03590-JEB, US District Court for the District Court of Columbia, Dec. 9, 2020 (Complaint for injunctive and other equitable relief). Available at https://www.ftc.gov/enforcement/cases-proceedings/191-0134/facebook-inc-ftc-v.

_____. **In the matter of Cambridge Analytica, LLC.** Docket No. 9383, File No. 1823107. Available at https://www.ftc.gov/enforcement/cases-proceedings/182-3107/cambridge-analytica-llc-matter.

_____. **In the Matter of Dell Computer Corp.** Docket No. C-3658, File No. 931 0097. Available at https://www.ftc.gov/enforcement/cases-proceedings/931-0097/dell-computer-corporation.

_____.**In the Matter of Eli Lilly and Co.**, Docket No.C-4047, File No. 0123214 Available at https://www.ftc.gov/sites/default/files/documents/cases/2002/05/elilillycmp.htm.

_____.**In the Matter of Facebook, Inc.** Docket No. C-4365, File No. 0923184. Available at https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc.

_____. **In the Matter of Facebook, Inc.**, FTC File No. 092 3184. Available at https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc.

_____.**In the Matter of Facebook, Inc.,** Civil Action No. 19-cv-2184. Available at https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf.

_____.**In the Matter of Gateway Learning Corp.**, FTC File No. 042 3047. Available at https://www.ftc.gov/enforcement/cases-proceedings/042-3047/gateway-learning-corp-matter.

_____. **In the Matter of GeoCities**. Docket No. C-3850, File No. 9823015, Available at https://www.ftc.gov/sites/default/files/documents/cases/1999/02/9823015cmp.htm.

_____.**In the Matter of Google, Inc.** Docket No. C-4336, File No. 1023136. Available at https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzcmpt.pdf.

_____.**In the Matter of Google Inc**., File No. 111-0163 Jan. 3, 2013 (Statement of the Federal Trade Commission Regarding Google's Search Practices) Available at https://www.ftc.gov/public-statements/2013/01/statement-federal-trade-commission-regarding-googles-search-practices.

_____.**In the matter of Google Inc.,** File No. 111-0163 Jan. 3, 2013 (Statement of Commissioner Maureen K. Ohlhausen) Available at https://www.ftc.gov/public-statements/2013/01/separate-statement-commissioner-maureen-ohlhausen-matter-google-inc.

_____.**Google/DoubleClick.** File No. 071-0170. (Statement of Federal Trade Commission) Available at https://www.ftc.gov/public-statements/2007/12/statement-federal-trade-commission-concerning-googledoubleclick.

_____.**Google/DoubleClick**, File No. 071-0170. (Dissenting Statement of Commissioner Pamela Jones Harbour) Available at https://www.ftc.gov/public-statements/2007/12/dissenting-statement-commissioner-harbour-matter-googledoubleclick.

_____.**In the Matter of Intel Corp.** Docket No. 9341, File No. 0610247. Available at https://www.ftc.gov/enforcement/cases-proceedings/061-0247/intel-corporation-matter.

_____. **In the Matter of Motorola Mobility LLC and Google, Inc.**, Docket No. C-4410, File No. 1210120, Jan. 3, 2013. Available at https://www.ftc.gov/enforcement/cases-proceedings/1210120/motorola-mobility-llc-google-inc-matter.

_____. ***In re*** **Negotiated Data Solutions LLC**, File No. 051-0094. Available at https://www.ftc.gov/enforcement/cases-proceedings/051-0094/negotiated-data-solutions-llc-matter.

_____. **In the Matter of Nomi Technologies, Inc.** Docket No. C-4538, File No. 1323251. Available at https://www.ftc.gov/system/files/documents/cases/150902nomitechcmpt.pdf.

_____. **In the Matter of Sears Holding Management Corp.** Docket No. C-4264, File No. 0823099. Available at https://www.ftc.gov/sites/default/files/documents/cases/2009/09/090604searscmpt.pdf.

_____.**In the matter of Snapchat.** Docket No. C-4501, File No. 1323078. Available at https://www.ftc.gov/enforcement/cases-proceedings/132-3078/snapchat-inc-matter.

_____. **In the matter of Uber Technologies, Inc.** Docket No. C-4662, File No. 1523054. Available at https://www.ftc.gov/enforcement/cases-proceedings/152-3054/uber-technologies-inc

_____. **In the Matter of Vision I Properties, LLC et al.** Docket No. C-4135, File No. 0423068, Apr. 26, 2005. Available at https://www.ftc.gov/enforcement/cases-proceedings/042-3068/vision-i-properties-llc-et-al-matter.

_____.**Joint statement of FTC commissioners Chopra, Slaughter, and Wilson regarding social media and video streaming service providers' privacy practices**. File No. P205402 Dec. 14, 2020. Available at https://www.ftc.gov/public-statements/2020/12/joint-statement-ftc-commissioners-chopra-slaughter-wilson-regarding-social.

_____. **Letter from Jessica L. Rich, Director of the Federal Trade Commission Bureau of Consumer Protection to Erin Egan, Chief Privacy Officer, Facebook, and to Anne Hoge, General Counsel, WhatsApp Inc.** Apr. 10, 2014. Available at https://www.ftc.gov/public-statements/2014/04/letter-jessica-l-rich-director-federal-trade-commission-bureau-consumer.

_____.**Premerger Notification Program**. [Washington], [s.d.]. Available at https://www.ftc.gov/enforcement/premerger-notification-program. Last access on May 06, 2021.

_____. **Protecting consumer privacy in an era of rapid change: recommendations for business and policymakers**, Washington: [s.n.], Mar. 2012 Available at https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

_____. **United States v. Path, Inc.** Case 3:13-cv-0448 (Northern District of Cal. Aug. 2, 2013) (consent decree and order for civil penalties, permanent injunction and other relief) https://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathincdo.pdf.

_____. **Statement of Enforcement Principles Regarding "Unfair Methods of Competition" Under Section 5 of the FTC Act.** Washington, Aug. 13, 2015. Available at https://www.ftc.gov/system/files/documents/public_statements/735201/150813section5enforcement.pdf.

_____. **Statement from FTC Chairwoman Edith Ramirez on Appellate Ruling in the Wyndham Hotels and Resorts Matter**. [Washington], Aug. 24, 2015. Available at https://www.ftc.gov/news-events/press-releases/2015/08/statement-ftc-chairwoman-edith-ramirez-appellate-ruling-wyndham.

FOUCAULT, Michel. **Discipline and punish: the birth of the prison**, translated by Alan Sheridan. New York: Pantheon, 1977.

FOURCADE. Marion; HEALY, Kieran. Seeing like a market. **Socio-Economic Review**, 2017, Vol. 15, No. 1, 9–29, doi: 10.1093/ser/mww033.

FRIEDEN, Rob. The Internet of platforms and two-sided markets: implications for competition and consumers. **Villanova Law Review**, v. 63, n. 2, p. 269–320, 2018.

FUKUYAMA, Francis et al. **Report of the working group on platform scale**. Stanford: [s.n.], 2020. Available at https://cyber.fsi.stanford.edu/publication/report-working-group-platform-scale. Last access on Jan. 3, 2021.

GARTENBERG, Chaim. Epic's Fortnite standoff is putting Apple's cash cow at risk. **The Verge**, August 17 2020. Available at https://www.theverge.com/2020/8/17/21369460/apple-fortnite-app-store-services-business-model-epic-games. Last access Aug. 25, 2020.

GILBERT, Ben. 'Fortnite' made $1.8 billion in 2019, analysts say – that's down 28% from 2018, but it's still the biggest game in the world. **Business Insider** January 3, 2020. Available at <https://www.businessinsider.com/how-much-did-fortnite-make-in-2019-2020-1>. Last access on Aug. 25, 2020.

GILLESPIE, Tarleton. The politics of ' platforms '. **News Media & Society**, v. 12, n. 3, p. 347–363, 2010.

GASSER, Urs; PALFREY, John G. Breaking down digital barriers: when and how ICT interoperability drives innovation. **Berkman Center Publication Series**, 2007. Available at <https://dash.harvard.edu/bitstream/handle/1/2710237/Breaking%20Down%20Digital%20Barriers.pdf?sequence=2&isAllowed=y>.Last access Aug. 17, 2020.

GOBRY, Pascal-Emmanuel. Eric Schmidt To World Leaders At eG8: Don't Regulate Us, Or Else. **Business Insider**, [s.l.] May 24, 2011. Available at https://www.businessinsider.com/eric-schmidt-google-eg8-2011-5. Access on Aug 18, 2020.

GLAESER; SHLEIFER, The Rise of the Regulatory State. **Journal of Economic Literature**, v. 41, p. 401-425, 2003.

GYUNN, Jessica. Delete Facebook? It is a lot more complicated than that, **USA Today**. [s.l.] Mar 28 2018. Available at https://www.usatoday.com/story/tech/news/2018/03/28/people-really-deleting-their-facebook-accounts-its-complicated/464109002/. Last access on May 30, 2021.

HAGGERTY, Kevin D; ERICSON, Richard V, The surveillant assemblage, **The British Journal of Sociology**, v. 4, n. 51, p. 605–622, 2000.

HAMILTON, Robert W. Procedures for the adoption of rules of general applicability: the need for procedural innovation in administrative rulemaking. **California Law Review**, v. 60, p. 1276–1338, 1972.

HANS, G. S., Privacy Policies, Terms of Service and FTC Enforcement: broadening unfairness regulation for a new era, **Michigan Telecommunications & Technology Law Review**, v. 19, n. 1, p. 163–197, 2012.

HARTZOG, Woodrow; SOLOVE, Daniel J, The Scope and Potential of FTC Data Protection, **The George Washington Law Review**, v. 83, n. 6, p. 2230–2300, 2015.

HAYES, Ben, The surveillance industrial complex, in: BALL, KIRSTIE; HAGGERTY, KEVIN; LYON, David (Org.), **Routledge Handbook of Surveillance Studies**, New York: Routledge, 2012.

HETCHER, Steven. The De Facto Federal Privacy Commission, **Journal of Computer & Information Law**. v. 19, n. 1, 2000.

HILL, Kashmir. How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did, **Forbes**, [s.l.] Feb. 16 2012. Available at https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#4f9f5efb6668. Last access on Oct. 2, 2020.

HOOFNAGLE, Chris Jay. Assessing the Federal Trade Commission ' s privacy assessments. **IEEE Security & Privacy**, v. 14, n. 2, p. 58–64, 2016. Available at https://www.computer.org/cms/Computer.org/ComputingNow/docs/ieeesecurity-and-privacy-assessing-federal-trade-commissions-privacyassessments.pdf.

_____. **Federal Trade Commission privacy law and policy**, New York: Cambridge University Press, 2016.

_____. FTC Regulation of Cybersecurity and Surveillance, in: GRAY, David; HENDERSON, Stephen E. (Orgs.), **The Cambridge Handbook of Surveillance Law**, New York: Cambridge University Press, 2017.

HOOFNAGLE, Chris Jay; HARTZOG, Woodrow; SOLOVE, Daniel J., The FTC can rise to the privacy challenge, but not without help from Congress. **Brookings.** [s.l.], Aug. 8, 2019. Available at: <https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/> Last access on June 10, 2021.

HOVENKAMP, Herbert, The Federal Trade Commission and the Sherman Act, **Florida Law Review**, v. 62, p. 1–23, 2010.

JOHNSON, David R.; POST, David, Law and Borders : The Rise of Law in Cyberspace, **Stanford Law Review**, v. 48, n. 5, p. 1367–1402, 1996.

KAPCZYNSKI, Amy. The Law of Informational Capitalism. **Yale Law Journal**, p. 1460–1515, 2020.

KERBER, Wolfogang; SCHWEITZER, Heike. **Interoperability in the digital economy**. **JIPITEC** v. 8, 2017, 39-58.

KEYS, Mattew. A brief history of Facebook's ever-changing privacy policies, **Medium.** [s.l.] Mar. 21, 2018, https://medium.com/@matthewkeys/a-brief-history-of-facebooks-ever-changing-privacy-settings-8167dadd3bd0. Last access May 13, 2021.

KHARPAL, Arjun. China's move to regulate its tech giants is part of its bigger push to become a tech 'superpower', **CNBC,** [s.l.], Jan 12 2021, Available at https://www.cnbc.com/2021/01/11/chinas-tech-regulation-part-of-bigger-push-to-become-a-superpower-.html. Last access on May 30, 2021.

KINCAID, Jaso. The Facebook privacy fiasco begins. **Techcrunch.** [s.l.] Dec. 10, 2009. Available at https://techcrunch.com/2009/12/09/facebook-privacy/. Last access May 13, 2021.

KOVACIC; WINERMAN, Competition policy and the application of section 5 of the Federal Trade Commission Act. **Antitrust Law Journal**, v. 76, n. 3, p. 929-950, 2010.

LAIDLAW, Emily. A Framework for Identifying Internet Information Gatekeepers. International Review of Law, Computers & Technology, v. 24, n. 3, p. 1–16, 2010.

LASTOWKA, Greg. Google's Law, **Brooklyn Law Review**. v. 73, n. 4, p. 1327–1410, 2008

LAWSKY, David. Google closes DoubleClick merger after EU approval, **Reuters** [s.l.], Mar. 11 2008. Available at https://www.reuters.com/article/us-google-doubleclick-eu-idUSBFA00058020080311.

LESSIG, Lawrence. **Code and Other Laws of Cyberspace ver. 2.0**. New York: Basic Books, 2006.

LIND, Data. Facebook "I voted" sticker was a secret experiment on its users, **Vox** Nov 4, 2014. Available at https://www.vox.com/2014/11/4/7154641/midterm-elections-2014-voted-facebook-friends-vote-polls. Access on Apr. 12, 2021.

LIPSMAN, Andrew. Global Ecommerce 2019: ecommerce continues strong gains amid global economic uncertainty. **Emarketer**, [s.l.], Jun. 27 2019. Available at <https://www.emarketer.com/content/global-ecommerce-2019>. Last access Jun 19, 2020.

LIST of mergers and acquisitions by Facebook, **Wikipedia: the free encyclopedia**. Available at https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Facebook. Access on May 18, 2021.

LITMAN, Jessica. Information privacy / information property. **Stanford Law Review**, v. 52, n. 5, p. 1283–1313, 2000.

LUBBERS, Jeffrey S, It's Time to remove the "mossified " procedures for FTC rulemaking, **The George Washington Law Review**, v. 83, n. 6, p. 1979–1998, 2015.

LYON, David. **Surveillance studies: an overview.** Cambridge: Polity, 2007.

LYNSKEY, Orla. Regulating ' Platform Power '. **LSE Law, Society and Economy Working Papers No. 1/2017**. Available at < https://ssrn.com/abstract=2921021>.

MAJONE, Giandomenico. Do estado positivo ao estado regulador: causas e consequências da mudança no modo de governança. **Revista Do Serviço Público**, v. 50, n. 1, p. 5-36. Available at https://doi.org/10.21874/rsp.v50i1.339. Last access on Aug. 30, 2020.

MANOKHA, Ivan. Surveillance: The DNA of platform capital — The case of Cambridge Analytica put into perspective, **Theory and Event**, v. 21, n. 4, p. 891–913, 2018.

MCDONALD, Aleecia; CRANOR, Lorrie Faith. The Cost of Reading Privacy Policies. **Journal of Law and Policy for the Information Society**, v. 4. N. 3, 543-568, p. 565, 2008.

TERRELL, McSweeny. FTC 2.0: Keeping Pace with Online Platforms. **Berkeley Technology Law Journal**, v. 32, 1027-1050, 2017.

MOE, Terry M. The Politics of Bureaucratic Structure. *In*: CHUBB, John E.; PETERSON, Paul E. (Orgs.), **Can the Government Govern?**, Washington: The Brookings Institution, 1989, p. 267–329.

MEYER, Robinson. Everything we know about Facebook's secret manipulation experiment. **The Atlantic**. [s.l.], Jun. 28 2014. Available at https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/. Last access Mar. 30, 2021.

MOLLA, Rani. Google, Amazon, and Facebook all spent record amounts last year lobbying the US government. **Vox**, [s.l.] Jan. 23. 2019. Available at https://www.vox.com/2019/1/23/18194328/google-amazon-facebook-lobby-record. Last access on Aug. 18, 2020.

MONAHAN, Torin; WOOD, David Murakami, Introduction: surveillance studies as a transdisciplinary endeavour. *In*: MONAHAN, Torin; WOOD, David Murakami (Orgs.), **Surveillance Studies - A Reader**, New York: Oxford University Press, 2018.

MOROZOV, Evgeny. The real privacy problem, **MIT Technology Review**, v. 118, n. 8, p. 33–43, 2013.

_____. Facebook invades your personality, not your privacy. **Financial Times**. [s.l.]Aug. 10 2014. Available at https://www.ft.com/content/dd5e5514-198d-11e4-8730-00144feabdc0. Last access May 25, 2021.

MORTON, Fiona M Scott; DINIELLI, David C, Roadmap for an Antitrust Case Against Facebook. **Omidyar Network.** June 2020.

MUELLER, Milton. Digital Convergence and its Consequences, **Javnost - The Public**, 6:3, 11-27, https://doi.org/10.1080/13183222.1999.11008716.

MURRAY, Andrew D. Nodes and gravity in vitual space. **International Journal of the Study of Legislation**, v. 5, n. 1, p. 195–221, 2001.

_____. **Information Technology Law: The law and society**. 2 ed. Oxford: Oxford University Press, 2013.

NEHF, James P. The FTC 's proposed framework for privacy protection online : a move toward substantive controls or just more notice and choice ? **William Mitchell Law Review**, v. 37, n. 4, p. 1727–1744, 2011.

PRESS, Gil. Why Facebook triumphed over all other social networks. **Forbes**. [s.l.] Apr. 8, 2018. Available at https://www.forbes.com/sites/gilpress/2018/04/08/why-facebook-triumphed-over-all-other-social-networks/?sh=3e7e3af76e91 . Last access May 13, 2021.

OKULIAR, Alexander P.; OHLHAUSEN, Maureen K., Competition, consumer protection, and the right [approach] to privacy, **Antitrust Law Journal**, v. 80, n. 1, p. 121–156, 2015.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). **An introduction to online platforms and their role in the digital transformation**, Paris: OECD Publishing, 2019, p. 11. Available at https://doi.org/10.1787/53e5f593-en. Last access on Jun. 1 2021.

PASQUALE, Frank. The black boz society: The secret algorithms that control money and information. Cambridge: Harvard Unitersity Press, 2015.

_____. Two narratives of platform capitalism, **Yale Law & Policy Review**, v. 35, p. 309–320, 2016.

PERRIN, Andrew; ATSKE, Sara. About three-in-ten U.S. adults say they are 'almost constantly' online, **Pew Research Center**, [s.l.], 26 Mar. 2021. Available at https://www.pewresearch.org/fact-tank/2021/03/26/about-three-in-ten-u-s-adults-say-they-are-almost-constantly-online/. Last access on Jun 1 2021.

PRESS, Gil. Why Facebook triumphed over all other social networks. **Forbes**. [s.l.] Apr. 8, 2018. Available at https://www.forbes.com/sites/gilpress/2018/04/08/why-facebook-triumphed-over-all-other-social-networks/?sh=3e7e3af76e91 . Last access May 13, 2021.

REIDENBERG, Joel R. Governing Networks and Rule-Making in Cyberspace. **Emory Law Journal**, v. 45, p. 911-930, 1996.

_____. Lex Informatica : The Formulation of Information Policy Rules through Technology. **Texas Law Review**, v. 76, n. 3, p. 553–593, 1998.

REYES, Mariel Soto. Google, Facebook, and Amazon will account for nearly two-thirds of total US digital ad spending this year. **Business Insider**, [s.l.] Dec. 3 2020. Available at https://www.businessinsider.com/google-facebook-amazon-were-biggest-ad-revenue-winners-this-year-2020-12. Access on Apr. 27, 2021.

ROMM, Tony, Google dodges bullet in FTC probe, **Politico**, Jan 3, 2013. Available at https://www.politico.com/story/2013/01/google-dodges-bullet-as-ftc-closes-probe-085724.

ROSENCRANCE, Linda. Privacy groups say Google Double-Click merger will hurt consumers. **Computer World**, [s.l.] Dec 20 2007. Available at https://www.computerworld.com/article/2538252/privacy-groups-say-google-doubleclick-merger-will-hurt-consumers.html.

RUDDEN, Jennifer. Number of card transaction worldwide in 2019, by brand. **Statista,** [s.l.], Aug. 7 2020. Available at <https://www.statista.com/statistics/261327/number-of-per-card-credit-card-transactions-worldwide-by-brand-as-of-2011/>. Last access Jun 19, 2020.

RULE, James B., **Private lives and public surveillance: social control in the computer age**, London: Allen Lane, 1973.

RUSLI, Evelyn M. Facebook buys Instagram for $1 Billion, Dealbook. **New York Times,** [New York], Apr. 9 2012. Available at https://dealbook.nytimes.com/2012/04/09/facebook-buys-instagram-for-1-billion/.

SATARIANO, Adam. Big fines and strict rules unveiled against 'Big Tech' in Europe, **New York Times**, New York, Dec. 15 2020. Available at https://www.nytimes.com/2020/12/15/technology/big-tech-regulation-europe.html. Last access on May 30, 2021.

SCHONFELD, Erick. **Zuckerberg on who owns user data on Facebook: it's complicated**, **Techcrunch.** [s.l.] Feb. 16, 2009. Available at https://techcrunch.com/2009/02/16/zuckerberg-on-who-owns-user-data-on-facebook-its-complicated-2/ Last access May 13, 2021.

SCHWARTZ, Paul M. Property, privacy, and personal data. **Harvard Law Review**, v. 117, n. 7, p. 2056–2128, 2004.

SERWIN, Andrew B. The Federal Trade Commission and privacy: defining enforcement and encouraging the adoption of best practices. **San Diego Law Review**, v. 48, n. 809, p. 809–856, 2011.

SHIFFMAN, Betsy. Facebook CEO Apologizes, Lets Users Turn Off Beacon. **Wired.** [s.l.] May 12, 2007. Available at https://www.wired.com/2007/12/facebook-ceo-apologizes-lets-users-turn-off-beacon/.

SMARTPHONE market share. **IDC** Apr. 28 2021. Available at https://www.idc.com/promo/smartphone-market-share/os. Last access Jun 4, 2021.

SOCIAL Media Fact Sheet, Pew Research Center. [s.l.] Apr. 7, 2021. Available at https://www.pewresearch.org/internet/fact-sheet/social-media/#how-often-americans-use-social-media-sites. Last access May 30, 2021.

SOKOL, D Daniel; COMERFORD, Roisin, Antitrust and regulating big data, **George Mason Law Review**, v. 23, n. 5, p. 1129–1161, 2016.

SOLOVE, Daniel J. **The Digital Person: Technology and Privacy in the Information Age**. 1 ed., New York: New York University Press, 2004 SOLOVE, Daniel J. **The Digital Person: Technology and Privacy in the Information Age**. 1 ed., New York: New York University Press, 2004.

_____. A taxonomy of privacy, **University of Pennsylvania Law Review**, v. 154, n. 3, p. 477–560, 2006.

_____. **Understanding privacy**, Cambridge: Harvard University Press, 2008.

SOLOVE, Daniel J.; HARTZOG, Woodrow. The FTC and the new common law of privacy, **Columbia Law Review**, v. 114, n. 3, p. 583–676, 2014.

SRINIVASAN, Dina. The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy. **Berkley Business Law Journal**, v. 16, n. 1, 39-101, 2019.

SRNICEK, Nick. **Platform Capitalism**. Cambridge, UK: Polity Press, 2017.

_____. The challenges of platform capitalism, **Juncture,** v. 23, n. 4, p. 254–257, 2017.

STARR, Paul, How Neoliberal Policy Shaped the Internet – and What to Do About It Now. **The American Prospect,** [s.l.] Oct. 2 2019. Available at https://prospect.org/power/how-neoliberal-policy-shaped-internet-surveillance-monopoly/. Access on Aug 18, 2020.

STATT, Nick. Apple just kicked Fortnite off the App Store. **The Verge**, Aug. 13, 2020. Available at https://www.theverge.com/2020/8/13/21366438/apple-fortnite-ios-app-store-violations-epic-payments. Last access on Aug. 25, 2020.

STOLLER, Daniel R. Facebook, Google Fund Groups Shaping Federal Privacy Debate (3). **Bloomberg Law**, [s.l.] Nov. 18, 2019, https://news.bloomberglaw.com/privacy-and-data-security/facebook-google-donate-heavily-to-privacy-advocacy-groups. Access on Aug. 18, 2020.

STORY, Louise and HELFT, Miguel, Google buys DoubleClick for $3.1 billion, **New York Times**, [New York], Apr 14 2007. Available at https://www.nytimes.com/2007/04/14/technology/14DoubleClick.html. Access on Feb. 18, 2020.

STRAUSS, Peter L.. **Administrative Justice in the United States**. Third edit. Durham: Carolina Academic Press, 2016.

STUCKE, Maurice E; GRUNES, Allen P, No mistake about it: the important role of antitrust in the era of big data, **University of Tennessee Legal Studies Research Paper No. 269**, 2015. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2600051.

SUNSTEIN, Cass, **After the Rights Revolution: Reconceiving the Regulatory State**, Cambridge: Harvard University Press, 1993.

TAYLOR, Emily, **The Privatization of Human Rights: Illusions of Consent, Automation and Neutrality**, Series Global Commission on Internet Governance Paper Series, Ontario: Center for International Governance Innovation and Chatham House, 2016.

THE FACEBOOK effect: social media dramatically boosts organ donor registration. John Hopkins Medicine, [s.l.], June 18, 2013. Available at https://www.hopkinsmedicine.org/news/media/releases/the_facebook_effect_social_media_dramatically_boosts_organ_donor_registration. Last access on Apr. 12, 2021.

THE WORLD'S Most Valuable Brands. **Forbes**, [s.l.] Apr. 4, 2020. Available at https://www.forbes.com/powerful-brands/list/. Last access Jun. 30, 2020.

UNITED STATES OF AMERICA. NY Court of Appeals. Thomas v. Winchester, 6 N.Y. 397 (1852). July 1852. Available at http://www.courts.state.ny.us/reporter/archives/thomas_winchester.htm.

_____. _____. MacPherson v. Buick Motor Co., 217 N.Y. 382, 111 N.E. 1050. (1916) First party: Donald C. MacPherson; Second party: Buick Motor Company. Available at http://www.courts.state.ny.us/reporter/archives/macpherson_buick.htm.

_____. Supreme Court. Abrams v. United States, 250 US 616 (1919). First party: Abrams. Second party: United States. Nov. 10, 1919. Available at < https://supreme.justia.com/cases/federal/us/250/616/>.

_____. _____. Humphey's Executor v. United States, 295 U.S. 602 (1935). May 27, 1935. Available at https://supreme.justia.com/cases/federal/us/295/602/.

_____. _____. Wiener v. United States, 357 U.S. 349 (1958). June 30, 1958. Available at https://supreme.justia.com/cases/federal/us/357/349/.

_____. _____. FTC v. Colgate-Palmolive Co., 380 US 374, 385 (1965). April 5, 1965. Available at https://supreme.justia.com/cases/federal/us/380/374/.

_____. _____. Vermont Yankee Nuclear Power Corp. v. Natural Resources Defense Council, 435 U.S. 519 (1978). Apr. 3, 1978. Available https://supreme.justia.com/cases/federal/us/435/519/.

_____. _____. FTC v. Sperry & Hutchinson Co. 405 U.S. 233 (1972). Available at https://supreme.justia.com/cases/federal/us/405/233/.

_____. _____. Motor Vehicle Manufacturers Association of the United States, Inc. v. State Farm Mutual Automobile Insurance Company, 463 U.S. 29 (1983), June 24, 1983. Available at https://supreme.justia.com/cases/federal/us/463/29/.

_____. United States Court of Appeals, Tenth Circuit. FTC v. Accusearch Inc., 570 F. 3d 1187 (2009). Jun. 29, 2009. Available at https://bit.ly/3iCnfjw.

_____. _____.Third Circuit. FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (2015). Aug. 24, 2015. Available at https://caselaw.findlaw.com/us-3rd-circuit/1711436.html.

_____. UNITED STATES CODE. Title 5. Ch. 5, Subchapter II, §§551-59, Administrative Procedure Act. Available at https://www.law.cornell.edu/uscode/text/5/part-I/chapter-5/subchapter-II.

_____. _____. Title 15, Ch. 1, §§1-7, Sherman Act. Available at https://www.law.cornell.edu/uscode/text/15/chapter-1.

_____._____.Title 15, Ch. 1, §§12-27; Title 29, Ch. 5, §§52-53, Clayton Act. Available at https://www.law.cornell.edu/uscode/text/15/chapter-1.

_____. _____.Title 15, Ch. 2, §§41-58, Federal Trade Commission Act (FTC Act). Available at https://www.ftc.gov/sites/default/files/documents/statutes/federal-trade-commission-act/ftc_act_incorporatingus_safe_web_act.pdf.

_____. _____.Title 15 §§2301-2312, Magnuson-Moss Warranty—Federal Trade Commission Improvement Act. Available at https://www.ftc.gov/enforcement/statutes/magnuson-moss-warranty-federal-trade-commission-improvements-act.

_____. _____.Title 15 §§ 6501-6506, Children's Online Privacy Protection Act. Available at https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

_____. _____.Title 15 U.S.C. §§ 1681-1681x, Fair Credit Reporting Act Available at https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act.

_____. _____.Title 15 U.S.C § 6801-6827, Gramm-Leach-Biley Act. Available at https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act.

_____. _____.Title 15 U.S.C. § 6101-6108, Telemarketing and Consumer Fraud and Abuse Prevention Act. Available at https://www.ftc.gov/enforcement/statutes/telemarketing-consumer-fraud-abuse-prevention-act.

_____. _____.Title 18 U.S.C. § 1028, Identity Theft Assumption and Deterrence Act. Available at https://www.ftc.gov/enforcement/statutes/identity-theft-assumption-deterrence-act-1998.

VAN DIJCK, José; NIEBORG, David; POELL, Thomas. Reframing platform power. **Internet Policy Review**, v. 8, n. 2, p. 1–18, 2019.

VAN LOO, Rory, The missing regulatory state: monitoring businesses in an age of surveillance, **Vanderbilt Law Review**, v. 72, n. 5, p. 1563–1631, 2019.

VELLANTE, David. Breaking Analysis: How AWS, Azure and GCP Compete for Cloud Leadership in the 2020's. **Wikibon**, Feb. 9 2020, Available at https://wikibon.com/breaking-analysis-how-aws-azure-and-gcp-compete-for-cloud-leadership-in-the-2020s/. Last access on July 2, 2020.

WHATSAPP avisa que irá compartilhar dados dos usuários com o Facebook. **G1.** [s.l.] Jan. 6, 2021. Available at https://g1.globo.com/economia/tecnologia/noticia/2021/01/06/whatsapp-comeca-a-avisar-que-ira-compartilhar-dados-dos-usuarios-com-o-facebook.ghtml. Last access on May 30, 2021.

WHATSAPP inicia nova política de privacidade neste sábado; veja o que muda. **G1.** [s.l.] May 15, 2021. Available at https://g1.globo.com/economia/tecnologia/noticia/2021/05/15/whatsapp-inicia-nova-politica-de-privacidade-neste-sabado-veja-o-que-muda.ghtml.

WEBSTER, Frank. **Theories of the Information Society**, 3 ed., New York: Routledge, 2006.

WEBSTER, William R.. Public administration as surveillance. In: BALL, Kirstie; HAGGERTY, Kevin D; LYON, David (Orgs.), **Routledge Handbook of Surveillance Studies**, New York: Routledge, 2012.

WELLER, Toni. The information state: an historical perspective on surveillance. In: BALL, KIRSTIE; HAGGERTY, KEVIN; LYON, David (Org.), **Routledge Handbook of Surveillance Studies**, New York: Routledge, 2012.

WEST, Emily, Amazon: surveillance as a service, **Surveillance & Society**, v. 17, n. 1/2, p. 27–33, 2019.

WOOD, David Murakami; MONAHAN, Torin. Editorial: Platform surveillance, **Surveillance and Society**, v. 17, n. 1–2, p. 1–6, 2019.

WU, Tim, **Section 5 and 'unfair methods of competition': protecting competition or increasing uncertainty?**, Columbia Law & Economics Working Paper No. 542; Columbia Public Law Research Paper No. 14-508, 2016, Available at: https://scholarship.law.columbia.edu/faculty_scholarship/1961.

WU, Tim. **The curse of bigness: antitrust in the new Gilded Age**. New York: Columbia Global Reports, 2018.

WYATT, Edward. A Victory for Google as FTC takes no formal steps. **New York Times**, Jan 3, 2013. Available at https://www.nytimes.com/2013/01/04/technology/google-agrees-to-changes-in-search-ending-us-antitrust-inquiry.htm.

YIU, Tony, Why did Google buy DoubleClick?, **Towards Data Science,** [s.l.] May 6 2020. Available at https://towardsdatascience.com/why-did-google-buy-doubleclick-22e706e1fb07.

ZINGALES, Luigi; ROLNIK, Guy; LANCIER, Filippo Maria (Orgs.). **Stigler committee on digital platforms, Final Report**. [Chicago], September 2019. Available at https://research.chicagobooth.edu/stigler/media/news/committee-on-digitalplatforms-final-report. Last access on May 3, 2021.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism: the fight for a human future at the new frontier of power**. 1. ed, New York: PublicAffairs, 2019.