# MONITORING SURVEILLANCE CAPITALISM:

## ENABLING EMPOWERMENT TO DIGITAL CITIZENS

The National Executive Committee for Data Protection


APRIL 23, 2021

BOSTON UNIVERSITY

TEAM W CAPSTONE 2021: GROUP 7

Eliana Mugar

Danielle Park

Ali Harrison

Matt Cramer

Shiksha Nanda

Kaylan Comenole

## Table of Contents

# Glossary

## Term Abbreviations

**APPA:** American Privacy Protection Act (our proposed policy)

**CCPA:** California Consumer Privacy Act of 2018.

**COPPA:** The United States Children's Online Privacy Protection Act.

**EU/EEA:** The European Union and the European Economic Area.

**FCC**: Federal Communications Commission.

**FTC:** Federal Trade Commission.

**GDPR:** General Data Protection Regulation. This is a regulation in European Union law on data protection and privacy in the European Union and the European Economic Area.

**IDPCA:** South Korea's Infectious Disease Control and Prevention Act

**MERS:** Middle East Respiratory Syndrome

## Terms

**Behavior modification:** the way that behavior is altered through various techniques that encourage future actions and decisions.

**Big Data:** the large volume of structured and unstructured data.

**Datafication:** the transformation of aspects of people's lives into quantified data.

**Digital citizenship:** the self-enactment of people's role in society through the use of digital technologies.

**Nudging:** a form of choice that changes consumer behavior in a predictable manner that does not change economic incentives and choices.

**Privacy:** a claim, entitlement, or right of an individual to determine what information about themself may be communicated to others.

**Privacy policy:** a statement or legal document that discloses some or all of the ways a party gathers, uses, discloses, and manages a customer or client's data.

**Surveillance capitalism:** new economic conditions in which online information (data) is converted into valuable commodities, and where the capture and production of these commodities (data) rely on mass surveillance over the Internet.

**Abstract**

Surveillance Capitalism refers to a capitalist system that revolves around the commodification of individuals' data for the purpose of achieving profit. As the National Executive Committee for Data Protection (NECDP), we have written a report and policy proposal addressing the issues of surveillance capitalism. We discuss the history of surveillance capitalism, with a focus on its philosophy and the role of big data. We analyze the benefits of surveillance capitalism, particularly in terms of health care, and also examine the drawbacks, particularly the issues regarding election interference, violation of laws, and threats to cybersecurity. We review existing international models of legislation and also discuss the legislative challenges of formulating effective policy. Furthermore, since this is a policy paper, we will advocate for legislative reform, and include recommendations for intervening through an existing office in government.

## Introduction

Surveillance capitalism is a distinctly modern, though not inevitable, invention or development. Its two components, *surveillance* and *capitalism*, have both existed separately outside this compound, but pragmatic insights may be gained in analyzing their synthesis. To take an etymological approach, the word *surveillance* can be broken down into two parts: 'sur,' meaning "from above" and 'veillance,' meaning "to watch."[1] According to the Merriam-Webster Dictionary, capitalism can be defined as "an economic system characterized by private or corporate ownership of capital goods, by investments that are determined by private decision and by prices, production, and the distribution of goods that are determined mainly by competition in a free market."[2] When the two words are taken together: *surveillance capitalism*, they indicate a system in which surveillance — watching from above — is the means by which the ends characteristic of the capitalist system, namely, turning a profit, are achieved.

Surveillance, therefore, in this context, becomes the *modus operandi* of capitalism; it is a supremely contemporary way in which corporations make money. Nonetheless, there exists a power imbalance between the consumer and the corporation that allows for the corporation to exploit consumers and surveil them for the benefit of the company, and knowingly, at the expense of the consumer. If there is no regulation in this imbalanced and exploitative relationship, it can be presumed — and indeed, has been proven — that the companies themselves will not refrain from potentially ethically or politically distasteful courses of action to amass profit.

[1] Maša Galič, Tjerk Timan, and Bert-Jaap Koops, "Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation," *Philosophy & Technology* 30, (2017): 9-37. https://doi.org/10.1007/s13347-016-0219-1.

[2] *Merriam-Webster.com Dictionary*, s.v. "capitalism," accessed April 22, 2021, https://www.merriam-webster.com/dictionary/capitalism.

Clearly, there must be some solution offered to ensure the safety and privacy of the consumer, while simultaneously preserving the myriad of positive effects that have come from surveillance capitalism. As the National Executive Committee for Data Protection (NECDP), a report has been prepared addressing United States President Joseph Biden, outlining the issue to culminate in a policy proposal. The report will begin with the background of surveillance theories leading up to Shoshana Zuboff's landmark publication, *The Age of Surveillance Capitalism,* in which she originally coined the term 'surveillance capitalism,' the history of surveillance capitalism, and an analysis of the role that big data currently plays. Moving on, the report will discuss several case studies relating to the advantages and disadvantages of surveillance capitalism as well as their association with Zuboff. Then there will be a focus on creating legislation, where the report will address the challenges and various complications that come up with doing so. The report will examine several international models for creating such legislation. Finally, the report will conclude with a domestic policy proposal for how the US government should deal with the issue of surveillance capitalism. The policy will emphasize the role of and restore power to consumers, and will work to create the availability of options for users to survey their own data. Specifically, the policy will include a recommendation for a method of intervention through the means of an already existing government agency, the Federal Communications Commision (FCC), which would require government regulation of corporations and would ensure the protection of consumers' privacy.

## Background

### Philosophy of Surveillance

The major watershed in the history of surveillance theory is the concept of the Panopticon, created by English philosopher Jeremy Bentham and later developed and assayed by the French philosopher Michel Foucault. Surveillance theory can be divided into two chief components: Panoptical studies and post-Panoptical studies — the culmination of which will result in our understanding of Shoshana Zuboff's concept of 'surveillance capitalism.'

Prior to our modern conception of surveillance in terms of and structured by electronic technology, there existed theories of surveillance which depended on other methods of monitoring individuals for the use of some institution. In the late eighteenth century, Bentham devised a system that would attempt to surveil individuals with the goal of reforming their behavior to fit some standard, called the Panopticon.[3]

Bentham's Panopticon heavily relies on a form of architecture in which individuals are in a typically circular building and in the middle lies a central tower in which an inspector is present to monitor individuals from all possible angles [See Appendix A]. Since the individuals were surveilled at all times, they would obey the rules at all times, as well as conform to whatever standard was set before them.[4]

Bentham's Panopticon was later taken up by the 20th century French philosopher Michel Foucault, who twisted Bentham's original vision to an extent in his 1975 book, *Discipline and Punish*. Foucault defines *panopticism* as "a type of power that is applied to individuals in the form of continuous individual supervision, in the form of control, punishment, and

[3] Galič, Timan, and Koops, "Bentham, Deleuze and Beyond."
[4] Ibid.

compensation, and in the form of correction, that is, the modelling and transforming of individuals in terms of certain norms."[5] In analyzing Foucault's theory of *panopticism*, the most important word to keep in mind is *discipline*, which refers to the internalization and inculcation of surveillance in the individual.[6]

Foucault's panoptic 'disciplinary society' subjects individuals to normation and would make individuals docile and malleable, and thus, easily manipulated. It is in Foucault's theory that we see the beginning of a dualistic separation between the individual's actual being and corporeality, and their representation in society by those in power. Once an individual can be shaped by a society, that society has power over the individual and the individual becomes separated from itself. The metaphysical role of power structures in surveillance is one of the most important concepts in understanding surveillance capitalism and how it works.[7]

In the shift away from Bentham and Foucault into post-Panoptical theories of surveillance, there are a few key differences to understand. Later surveillance theories take a much more externalized route and put an emphasis on 'control' instead of 'discipline.' This shift comes primarily due to the idea that the "socio-technical landscape" that gave rise to the Foucauldian system of institutions and discipline has shifted since his time and that now a new theory of surveillance is required to understand how it works in a more contemporary setting.[8]

The most prominent of these post-Panoptical theories is Gilles Delueze's concept of 'control societies,' which he delineates in his 1990 essay "Postscript on the Societies of Control." Deleuze moves the Foucauldian emphasis on the individual to an approach that is more universal

[5] Galič, Timan, and Koops, "Bentham, Deleuze and Beyond."
[6] Ibid.
[7] Ibid.
[8] Ibid.

and generalized. On this point, it is helpful to address the modern phenomenon of globalization and the interconnectedness that is so present in our modern society, which is relevant to the role that social media plays in contemporary surveillance. 'Discipline,' Deleuze believes, is characteristic of an older society, but not the current one; it is instead 'control' that is more prevalent and significant today. Additionally, Deleuze insightfully shifts the focus away from governmental and institutional forms of surveillance and more towards that of corporations, noting that corporations are focused on controlling markets (not people) and that they usually do not have any other ulterior motives than a government might. For a corporation, the main goal of surveillance is clear: to make money. The distinction between 'discipline' and 'control' is further delineated: "Where discipline aims to achieve a long-term, stable and docile society striving for the optimal use of resources to reach government-issued goals, corporations focus on short-term results [i.e. profit]."[9] Nevertheless, in a 'control society,' continuous surveillance is still ever present, but it is distinctly more superficial than in a disciplinary society. It is noted that surveillance for 'control societies' becomes "abstract and numerical."[10] Deleuze further fleshes out what Foucault hinted at in this separation of the individual from their representation. Deleuze cleverly calls this representation of the individual a *dividual* and points out that it is not the individual that is surveilled, but is instead the *dividual* — the consumerist part of a person (or those data points) that is relevant to corporations in order to maximize profit.[11]

Building primarily on Deleuze's theories, Kevin D. Haggerty and Richard V. Ericson developed a theory in their 2000 essay "The Surveillant Assemblage." An association is drawn

[9] Galič, Timan, and Koops, "Bentham, Deleuze and Beyond."
[10] Ibid.
[11] Ibid.

between the Foucauldian Panopticon and the factories characteristic of industrial capitalism; the Panopticon illustrates a closed, physical space of surveillance. Conversely, Haggerty and Ericson focus on the modern shift towards a technological and electronic form of capitalism that is largely abstract, unstructured, and has no discrete boundaries, which affect the way surveillance is carried out.[12]

Their concept of 'surveillant assemblages' draws upon Deleuze's concept of an 'assemblage' — defined as a "'multiplicity of heterogenous objects, whose unity comes solely from the fact that these items function together, that they *work* together as a functional entity.'"[13] These 'heterogenous objects' can be made up of various things such as people, signs, chemicals, knowledge, or institutions. When taken together, the 'heterogenous objects' become 'flows' of stimuli or information — of which there is a surplus — that are then decoded and analyzed by 'surveillant assemblages.' Haggerty and Ericson mention two steps to surveillance: de-territorialization and re-assembly. It is through de-territorialization that the physical human body is abstracted from its data points; or, to use Deleuzean terms, it is through de-territorialization that the individual becomes a *dividual*. Then, once these 'flows' of information are extracted, they are re-assembled into a set of data points, or a 'data-double,' that becomes an "additional self, a 'functional hybrid,' serving foremost the purpose of being useful to institutions which allow or deny access to a multitude of domains (places, information, things) and discriminate between people."[14]

---

[12] K.D. Haggerty and R.V. Ericson (2000), "The surveillant assemblage," *The British Journal of Sociology*, 51: 605-622. https://doi.org/10.1080/00071310020015280.

[13] Ibid.

[14] Galič, Timan, and Koops, "Bentham, Deleuze and Beyond."

In a later paper, Haggerty critiques his own ideas and questions whether he has narrowed the scope of surveillance too much, acknowledging that there have contemporarily been an increase in the methods through which surveillance itself is accomplished, especially through unorthodox means. But, he also mentions that surveillance for the consumer can be enjoyable and may even be positive in many other contexts — examples include those advances found in science and in medicine that come from methods of surveillance. This serves to dilute Haggerty's original concept of 'surveillant assemblages' and to present surveillance as potentially less negative than was previously anticipated. Indeed, our report will show the positive effects of surveillance capitalism and part of our policy proposal will seek to preserve those.[15]

Shoshana Zuboff's landmark 2019 book *The Age of Surveillance Capitalism* — as well as several articles she wrote — outline her modern theory of surveillance capitalism. It is well-rooted in the previously discussed surveillance theories, but also ties in an element of neo-Marxism. Karl Marx believed that both economically and politically, surveillance is essential to the capitalist system. Reflective of Haggerty and Ericson's concepts and theories, Zuboff's theory seeks to go beyond them and establish surveillance as a fundamental and negatively dominating facet of capitalism and the society which it creates. Zuboff explains that there are benefits that come from capitalism in its origin, and that the laws of supply and demand were favorable for meeting the needs of the people as well as expanding democracy. It is, however, this new form of capitalism: *surveillance capitalism*, which corrupts this system, both

[15] Ibid.

economically and politically.[16] Zuboff presents a myriad of definitions for surveillance capitalism:

> (i) "A new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales"
> (ii) "A parasitic economic logic in which the production of goods and services is subordinated to a new global architecture of behavioral modification"
> (iii) "A rogue mutation of capitalism marked by concentrations of wealth, knowledge, and power unprecedented in human history"
> (iv) "The foundational framework of a surveillance economy"
> (v) "As significant a threat to human nature in the twenty-first century as industrial capitalism was to the natural world in the nineteenth and twentieth"
> (vi) "The origin of a new instrumentarian power that asserts dominance over society and presents startling challenges to market democracy"
> (vii) "A movement that aims to impose a new collective order based on total certainty"
> (viii) "An expropriation of critical human rights that is best understood as a coup from above: an overthrow of the people's sovereignty."[17]

Moreover, Zuboff's theory of surveillance capitalism has four key aspects. First, the role of big data and the ruthless mining for consumers' data, which breaks down the relationship between the corporation and the consumer in a process of de-personalization and de-humanization in this context. Second, and the most obvious, is surveillance of consumers and the subsequent modification of their behavior. Zuboff notes that "where power was previously identified with ownership of means of production, it is now constituted by ownership of means of behavioural modification."[18] Regulation of the people or entities with power (in this context, the corporations) is essential for balancing out this relationship and restoring power to the consumer, and because it is the corporations themselves that have the power, it is quite logical

[16] Keith Breckenridge, "Capitalism without Surveillance?," Review of *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, by Shoshana Zuboff. *Development and Change* 51, no. 3 (May 19, 2020): 921-935. https://doi-org.ezproxy.bu.edu/10.1111/dech.12588.

[17] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, (New York: PublicAffairs, 2019).

[18] Galič, Timan, and Koops, "Bentham, Deleuze and Beyond."

that it should be some extra-corporational entity that should regulate it, namely, the government. The report will address this in depth later on. Third is the role of personalized services such as ads. This indicates an imbalance in power, but also an imbalance of knowledge. The last aspect of Zuboff's theory is corporational experimentation in the market, which reveals causation (as opposed to just correlation) in the market itself as well as in consumer behavior.[19] An example of this would be the attempt to affect users' mood in secret by Facebook, and on this note, Zuboff says, "'reality' is subjected to commodification and monetization and reborn as 'behavior.'"[20]

Zuboff's presentation of surveillance capitalism is disconcerting, as it does not account for any privacy concerns of consumers. Zuboff acknowledges this, and while recognizing that her theory of surveillance capitalism requires additional research and development, she puts forth the idea that the institution of democracy itself is at risk due to surveillance capitalism.[21] This last point is debatable, but overall, her assessment of modern surveillance theory and its connection with the contemporary stage of capitalism is highly significant and will inform our further outlining of this issue as well as our final policy proposal.

## History of Surveillance Capitalism

The contemporary phase of capitalism can be traced back to the early twentieth century with the rise of mass production and standardization. Fordism, named after business mogul Henry Ford, is defined as the "basis of modern economic and social systems in the industrialized,

[19] Galič, Timan, and Koops, "Bentham, Deleuze and Beyond."
[20] Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology* 30, (April 4, 2015): 75-89, https://ssrn.com/abstract=2594754.
[21] Zuboff, *The Age of Surveillance Capitalism*.

standardized mass production and mass consumption."[22] It is a distinct stage of economic development which began in the US in the 1940s by virtue of Henry Ford, and soon spread all over the world. Fordism refers to the mode of economic growth that occurred in the post-war time period, and its associated political and social order in advanced capitalism. Under Fordism, mass consumption and mass production were coupled together to produce sustained economic growth and widespread material advancement.[23]

Major success for the Fordism movement stemmed from three major principles: the standardization of production, the use of assembly lines which allowed unskilled workers to contribute to production, and the increase of living wages paid to workers to ensure that they could afford to purchase products they helped to make. These principles, along with the simultaneously occurring technological revolution allowed for Fordism to flourish. When the 1970s recession put an end to the overall post-war economic expansion, the world economy had to be reinvented. Additionally, the rise of computer technology meant that mass production had to be completely redesigned. Thus, the concept of post-Fordism arose.[24] Post-Fordist theorists claim modern industrial production experienced a shift from mass production in large factories to specialized markets based on flexible production. This post-Fordist shift also mirrors the shift from the Foucauldian disciplinary societies to the Deleuzean control societies.

Fordism introduced a new logic of high-volume production at low cost per unit. Zuboff claims this logic can be seen in modern capitalism through the packaging of personal data and behavioral information and selling these data units to advertisers. Zuboff has coined this process

[22] Bob Jessop, "Fordism," Encyclopedia Britannica, last modified April 1, 2013, https://www.britannica.com/topic/Fordism.

[23] G. F. Thompson, "Fordism, Post-Fordism, and the Flexible System of Production," accessed April 22, 2021, https://www.cddc.vt.edu/digitalfordism/fordism_materials/thompson.htm.

[24] Rob Hudson, "Fordism," in *International encyclopedia of human geography. 7. Me - N* (2009), 226.

'surveillance capitalism.' Google was the first company to learn how to capture surplus behavioral data and use it to compute predictions as to what products customers would be interested in buying. They then sold that data to their customers, the advertisers. According to Zuboff, Google understood that users would be unlikely to agree to the translation of their experiences online into behavioral data. They were aware that their methods had to go undetected; in the early 2000s, Google turned to using advertising to their advantage when they faced pressure to transform their investments into earnings as they realized they did not have a product to sell. Similar to Ford, they employed a trial and error process and adapted their capabilities to a new direction as they began selling adverts based on personal information about their users. Additionally, Google was able to commodify their data to use their knowledge on customers to pair them with paying advertisers thus creating a new era of surveillance capitalism.[25]

## Big Data

Surveillance capitalism functions under the use of big data, an umbrella term involving scattered data. The challenge with big data is the process of transforming the raw data into relevant data — the representation of the individual which Deleuze has conceptualized as the *dividual*. In order for this transformation to occur, three main hurdles of big data called the 3 V's need to be conquered: volume, velocity, and variety. The sheer amount of raw data to be processed, the pace of data processing, and the highly diverse sources of data pose challenges in

[25] Johnathon Shaw, "The Watchers," Harvard Magazine, December 18, 2016, https://harvardmagazine.com/2017/01/the-watchers.

controlling big data.[26] When businesses and other data collectors overcome these challenges, processed data becomes a commodity.

Currently, common terminology for units of measurement to describe data for personal storage of information include kilobytes, megabytes, and gigabytes, but the volume of big data exceeds these units of measurement [See Appendix B]. The large volume of available data means storing this data is difficult. As of 2020, the yottabyte (a quadrillion gigabytes) has been the largest approved standard size of storage.[27] With the growing size of information, collectors want to amass the data. If they are unsure of what to do with it in the present, they will still have it for future uses and therefore, a backup of overloaded information. Many businesses are racing to capitalize on big data, but they are also collecting more data as they capitalize.[28] Collectors must continuously improve how they process the raw data and transform it into relevant data. To do so, companies figured out demand sensing, which "sorts out the flood of data in a structured way to recognize complex patterns…."[29] Corporations must figure out how to deal with the quick influx of surplus data and re-assemble it into only the most relevant data.

Since there are multiple forms of data files, the data needs to be managed into a structured format. Advancements have been made to manage the variety of big data; we are now able to import data into "universally accepted and usable formats such as Extensible Markup

---

[26] Doug Laney, "3D Data Management: Controlling Data Volume, Velocity, and Variety," *Gartner,* 2001. http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.

[27] "How much is 1 byte, kilobyte, megabyte, gigabyte, etc.?" *Computer Hope*, August 31, 2020. https://www.computerhope.com/issues/chspace.htm.

[28] John Foley, "As Big Data Explodes, Are You Ready For Yottabytes?" *Forbes*, June 21, 2013. https://www.forbes.com/sites/oracle/2013/06/21/as-big-data-explodes-are-you-ready-for-yottabytes/?sh=4d35ff635b3f.

[29] Ibid.

Language (XML)."[30] User data, which is considered to be the main currency and a product of surveillance capitalism, also comes from a variety of sources, including social media and the Internet.[31] In light of digital advertising, consumers' decision making has become less individualistic and more reliant on businesses and social media. Consequently, consumer privacy, which permits consumers to have the ability to determine what data is stored and collected, has become limited because there are no regulations in big tech.[32] This leads to organizations creating consumer-targeted advertisements to influence their decision making**.** As current US legislation stands, "there's no general federal law to protect privacy,"[33] but "a number of existing federal laws govern [p]rivacy [p]olicies for specific circumstances."[34] For example, data collectors are legally required to disclose to users their practices on protecting personal information by Federal Trade Commission (FTC) regulation. Omegle (a free online chat website) stated in its privacy policy they collect data such as chat messages, IP addresses, and webcam images. Through their "Terms of Service" which users must accept, Omegle outlined that users cannot obtain access to their own data, which Omegle stores for approximately 120 days, nor can the data be modified or deleted by user request.[35]

Many social media platforms are "mining the data," meaning they monitor, track, and collect users' information and data. Through social media, users can post information about

---

[30] Foley, "As Big Data Explodes, Are You Ready For Yottabytes?"

[31] "Sources of big data: Where does it come from?" *CloudMoyo*, accessed April 18, 2021. https://www.cloudmoyo.com/blog/data-architecture/what-is-big-data-and-where-it-comes-from/.

[32] "About the IAPP," *International Association of Privacy Professionals*, accessed April 22, 2021. https://iapp.org/about/what-is-privacy/.

[33] Kristen Cornett, " Companies tracking you on social media; How do they do it?" *Dayton247Now*, November 2, 2018. https://dayton247now.com/news/local/companies-stalking-you-on-social-media-how-you-can-control-what-they-know-about-you.

[34] "Privacy Policies are Legally Required," *Free Privacy Policy*, December 28, 2020. https://www.freeprivacypolicy.com/blog/privacy-policy-legally-required/#Privacy_Policies_In_The_United_States.

[35] "Privacy policy," *Omegle*, June 3, 2014. https://www.omegle.com/static/privacy.html.

themselves. Some social media companies track a vast amount of data that most users are largely unaware of which can reveal personal information and allow companies to develop inferences about a user.[36] Facebook is known for its data collection and online advertising. Facebook receives initial data through the "About Me" section and collects the remainder of it from searches, clicks, and likes.[37] Facebook allegedly has "special arrangements with more than 150 companies to share its members' personal data."[38] If the specific company pays to use Facebook's ad services, users' searches will automatically appear on users' feeds.[39]

Companies use collected data by building an algorithm to gain insight into users' identity and personal interests.[40] Furthermore, the data companies collect are used to create lists of categories about each user, which aim to target ads specifically relevant to them.[41] Zuboff asserts, "They can't use any of their targeting mechanisms unless they have so much data that they know who we are."[42] In turn, this extends into influencing people's behavior and gives social media companies an endless real-time feed of users' feelings, thoughts, reactions, and even location information.[43] Zuboff believes the creation of surveillance capitalism was a direct result of

---

[36] Jacob Silverman, "How Tech Companies Manipulate Our Personal Data," *The New York Times*, January 18, 2019. https://www.nytimes.com/2019/01/18/books/review/shoshana-zuboff-age-of-surveillance-capitalism.html.

[37] Cornett, "Companies tracking you."

[38] "Facebook's Data-Sharing Deals Exposed," *BBC News*, December 19, 2018. https://www.bbc.com/news/technology-46618582.

[39] Cornett, "Companies tracking you."

[40] Natasha Singer, "The Week in Tech: How Google and Facebook Spawned Surveillance Capitalism," *The New York Times*, January 18, 2019. https://www.nytimes.com/2019/01/18/technology/google-facebook-surveillance-capitalism.html.

[41] Ibid.

[42] Shoshana Zuboff, Guillaume Chaslot, and Ramesh Srinivasan, "The Perilous Power of Social Media Platforms," interview by Jonathan Chang and Meghna Chakrabarti, WBUR, NPR, Audio, 46:54, February 4, 2021. https://www.wbur.org/onpoint/2021/02/04/the-perilous-power-of-social-media-platforms.

[43] Ciara Wake, "3 Ways That Social Media Knows You Better Than Your Friends and Family Do," *Loyola University Maryland Emerging Media*, accessed April 16, 2021, https://www.loyola.edu/academics/emerging-media/blog/2017/3-ways-that-social-media-knows-you-better-than-your-friends-and-family-do#:~:text=By%20tracking%20users%20Facebook%2C%20Instagram,of%20what%20your%20interest%20are.&text=By%20using%20the%20location%20services,you%20are%20at%20all%20times.

targeted advertising and states that Google used data logs to predict consumer behavior instead of improving products.[44] Through big data analysis, targeted digital advertising does most of the decision making for consumers, by catering to consumers' predicted preferences.

Surveillance capitalists "soon discovered that they could use these data not only to know our behavior but also to shape it. . . .."[45] Digital advertising uses decision-making technologies to help shape consumer choices through automated systems that have the ability to receive data from consumer searches, favorite brands, and purchase history — the essence of behavior modification. These automated systems, similar to Haggerty and Ericson's concept of 'surveillant assemblages,' have the ability to influence consumer behavior through 'nudging.' According to big data researcher Karen Yeung, a 'nudge' is best defined as a form of choice that changes consumer behavior in a predictable manner that does not change economic incentives and choices.[46] Nudges can be as simple as encouraging healthy eating, or utilizing 'big data' to curate personalized playlists.

In surveillance capitalism, the creation of value relies on extracting data from users, transforming the extracted data into behavioral predictions of users, then monetizing the data and behavioral predictions through markets in which users cannot participate.[47] To create value from processed data, data collectors combine the data, use analytical methods, then form new relations, connections, patterns, and observed behaviors.[48] This process, otherwise known as

---

[44] Zuboff, Chaslot, and Srinivasan, "The Perilous Power of Social Media Platforms."

[45] Zuboff, "'Surveillance Capitalism Has Gone Rogue."

[46] Karen Yeung, "'Hypernudge': Big Data as a mode of regulation by design," *Information, Communication & Society* 20, no. 1 (2017): 118. https://doi.org/10.1080/1369118X.2016.1186713.

[47] Tuukka Lehtiniemi, "Personal Data Spaces: An Intervention in Surveillance Capitalism?" *Surveillance & Society* 15, no. 5 (2017): 627. https://doi.org/10.24908/ss.v15i5.6424.

[48] Bram Klievink, Bart-Jan Romijn, Scott Cunningham, and Hans de Bruijn, "Big Data in the Public Sector: Uncertainties and Readiness," *Information Systems Frontiers* 19, no. 2 (April 2017): 271. http://dx.doi.org.ezproxy.bu.edu/10.1007/s10796-016-9686-2.

'datafication.' With the influx of big data and its prominence in social media and advertising, companies with the capabilities to manage the 3 V's have been able to commodify collected data and turn it into a valuable currency in surveillance capitalism. As a result, there are specific big data processing businesses who are the innovators in big data processing technologies. Through 'datafication,' platform companies offer free services to users and "expect profits from customers in other markets, often including markets where they sell targeting to advertisers."[49] Because big data is managed within an ambiguous cyberspace, the information is available on the market for any entity capable of making the data useful.

Aside from the lack of user control on where the data goes, Zuboff mentions the existence of an asymmetric power structure regarding the data collection of users, asserting that "data extraction . . . is a one-way process that occurs in the absence of dialogue between companies and their users, despite data signaling personal and potentially intimate details about users."[50] This data collection power structure gives businesses and other data collectors the ability to control the data in a monopolistic manner.[51] Without user control, restricting access from outside data collectors remains complicated, which means data collectors can obtain user data with minimal consequence. The easy accessibility to user data and its high value for behavioral insights means big data collection needs to be monitored in surveillance capitalism.

[49] Lehtiniemi, "Personal Data Spaces," 627.
[50] Lehtiniemi, "Personal Data Spaces," 628.
[51] Ibid.

## Current US Legislation

Living in the age of surveillance capitalism, the primary point of concern is how data is accumulated and processed past what individuals have disclosed. Thus, data protection laws and regulations that protect individuals' fundamental rights to privacy are essential.[52] While the US does not have a single principal data protection legislation, there are sector-specific and industry-specific national privacy and data protection laws and regulations. These laws also apply to "financial institutions, telecommunications companies, personal health information, credit report information, children's information, telemarketing and direct marketing."[53]

Despite the lack of chief legislation in the US at the federal level, the US Federal Trade Commission (FTC) has authority over a wide range of commercial entities to protect consumers from unfair or deceptive practices. This includes the use of deceitful marketing methods as well as the failure to comply with its privacy regulations and negligence to provide sufficient security regarding personal information.[54] The United States government also has various privacy and data security laws across all 50 states and territories. These are provisions for "safeguarding data, disposal of data, privacy policies, appropriate use of Social Security numbers and data breach notification."[55]

State laws often impose restrictions on the collection, use, and disclosure of specific types of information. Each state in the US has occupied data breach notifications which is

---

[52] Imelda Rabang, "Living in the Age of Surveillance is a Modern-Day Threat," *Bold Business*, August 29, 2019. https://www.boldbusiness.com/digital/surveillance-capitalism/.

[53] *Law in the United States*, (Data Protection Laws of the World, 2021), last modified January 28, 2021, https://www.dlapiperdataprotection.com/index.html?t=law&c=US&c2=.

[54] Steven Chabinsky and F. P. Pittman, "Relevant Legislation and Competent Authorities," in USA: Data Protection Laws and Regulations (ICLG.com, 2020). https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa.

[55] *Law in the United States*.

applicable to particular types of personal data about residents. California, for example, has over 25 state privacy laws including the recently established California Consumer Privacy Act of 2018 (CCPA). The CCPA aims to give consumers more control over their personal information that is collected by businesses. CCPA regulations provide guidelines for law enforcement to secure new privacy rights for California residents, including:

- "The right to know about the personal information a business collects about them and how it is used and shared;
- The right to delete personal information collected from them (with some exceptions);
- The right to opt-out of the sale of their personal information; and
- The right to non-discrimination for exercising their CCPA right."[56]

Recently, there have been additions to the legal provisions regarding biometric data of individuals. Biometric data is defined as "personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or fingerprint data."[57] The Illinois Biometric Information Privacy Act (BIPA), enacted in 2018, was the first biometric data protection law in the US. Under this act, private entities that use biometric data are required to have a "written policy, schedule, and guideline on its retention, collection, and destruction."[58] What makes BIPA different from other regulations is its ability to provide private right of action, allowing individuals to directly file for a lawsuit for damages stemming from a violation of the act.

---

[56] *California Consumer Privacy Act (CCPA)*, (Office of the Attorney General, 2020). https://oag.ca.gov/privacy/ccpa.

[57] "Biometric Data Protection (GDPR, CCPA/CPRA)," *Thales*, last modified April 10, 2021, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data.

[58] Natalie A. Prescott, "The Anatomy of Biometric Laws: What US Companies Need To Know in 2020," *The National Law Review*, January 15, 2020. https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020.

## Benefits to Surveillance Capitalism

### Contact Tracing

Contact tracing is traditionally used in communities as a tool to identify those who have recently been infected with a virus, and interview them through their local health department. Individuals are asked to identify recently visited places and people they have come into close contact with.[59] In December 2019, a disease named COVID-19, caused by the SARS-CoV-2 virus, emerged.[60] In order to ensure the spread of COVID-19 is effectively suppressed, contact tracing has been used widely in many countries to identify and investigate those who have been exposed to the virus. Alongside this traditional approach to contact tracing, countries have also developed mobile apps to record travel history and track if one has been exposed to someone infected. South Korea is an example of utilizing a vigorous contact tracing system that has aided them in minimizing the outbreak of COVID-19.

In 2015, South Korea experienced the largest Middle East Respiratory Syndrome (MERS) Coronavirus outbreak outside the Middle East. After the MERS outbreak, South Korea implemented Article 76-2(2) of South Korea's Infectious Disease Control and Prevention Act (IDPCA).[61] This legislation granted the government abilities to obtain private data, with or without a warrant, from any patients and was created to contain any future viruses by implementing several precautionary/safety measures. Since the emergence of COVID-19, contact

[59] William F. Marshall, "Can Contact Tracing Stop Coronavirus?" *Mayo Clinic*, December 15, 2020. https://mayoclinic.org/diseases-conditions/coronavirus/expert-answers/covid-19-contact-tracing/faq-20488330.

[60] Lauren M. Sauer, "What Is Coronavirus?," *Johns Hopkins Medicine*, accessed April 22, 2021. https://www.hopkinsmedicine.org/health/conditions-and-diseases/coronavirus.

[61] Hakyung Kate Lee, "South Korea's Contact Tracing Sheds Light on Extensive Efforts to Slow Spread of COVID-19," *ABC News,* December 9, 2020. https://abcnews.go.com/International/south-koreas-contact-tracers-struggle-slow-spread-covid/story?id=74621480.

tracing in South Korea has been led, in part, by government designated officers called the Epidemics Intelligence Service (EIS). These officials are COVID-19 patients' first point of contact, and notify them of their diagnosis. These officers collect a detailed path of movement from the patients and do field research to ensure the validity of the information provided to them. Their field research includes cross-checking the testimonies provided by patients, and the penalty for fabricating the truth is high under the Infectious Diseases Control and Preventions Act.[62] These measures range from alerting citizens of nearby cases through text messages to creating a government-mandated GPS-tracking app to monitor and punish people who break quarantine.[63] Through these measures, the government was able to record the locations of every patient by "extract[ing] surveillance footage, credit card histories and cellular geolocation data of both confirmed and potential patients without a warrant."[64] The South Korean government justifies the publication of information as they believe that "the public is more likely to trust it if it releases transparent and accurate information about the virus." [65]

South Korea's ability to do a thorough epidemiology investigation on every patient has been praised, as the World Health Organization (WHO) claims that their efforts have helped to significantly reduce the spread of the virus. Contact tracing in South Korea is mandated by the law, unlike in the US, where authorities rely on word of mouth through interviews with patients and "opt-in" phone tracking apps. More specifically, the US Constitution states that health authorities do not have the legal power to "shut down religious gatherings or to extract

[62] Lee, "South Korea's Contact Tracing."

[63] George Baca, "Eastern surveillance, Western malaise, and South Korea's COVID-19 response: oligarchic power in Hell Joseon," *Dialectical Anthropology* 44, (August 24, 2020): 301-307. https://doi.org/10.1007/s10624-020-09609-y.

[64] Ibid.

[65] Mark Zastrow, "South Korea is Reporting Intimate Details of COVID-19 Cases: Has It Helped?" *Nature*, March 18, 2020. https://www.nature.com/articles/d41586-020-00740-y.

geolocation data. . . … for contact-tracing without a warrant,"[66] as the Fourth Amendment prohibits any unreasonable searches and seizures. Additionally, because it is not a federal government matter, every state has a different approach or guideline to every health crisis. Ultimately, the use of an integrated technological system to help epidemiological investigators track the spread of the virus have helped authorities in South Korea immensely; the aggressive nature of their contact tracing methods have been justified.[67]

## Innovation and the Health Care Sector

Within surveillance capitalism, the commodification of big data has led many companies, sectors, and industries to technologically advance. The analysis of big data can provide potential benefits of facilitating the development of new, personalized services, improving traditional manufacturing industries, and advancing the health care sector.[68] One example for the development of new, personalized services would be the data collection of geospatial data to provide real-time traffic updates.[69] By collecting personal data through tracking sensors on phones or vehicles, tracking areas of road congestion can aid GPS systems to reroute based on car density.

---

[66] Jung Won Sonn, "Coronavirus: South Korea's success in controlling disease is due to its acceptance of surveillance," The Conversation, March 19, 2020. https://theconversation.com/coronavirus-south-koreas-success-in-controlling-disease-is-due-to-its-acceptance-of-surveillance-134068.

[67] Sangchul Park, Gina J. Choi, and Haksoo Ko, "Information Technology–Based Tracing Strategy in Response to COVID-19 in South Korea—Privacy Controversies," *Jama Network*, April 2020. https://jamanetwork.com/journals/jama/fullarticle/2765252.

[68] Thomas Niebel, Fabienne Rasel, and Steffen Viete, "BIG data—BIG gains? Understanding the link between big data analytics and innovation," *Economics of Innovation and New Technology* 28, no. 3 (2019): 297. https://doi.org/10.1080/10438599.2018.1493075.

[69] Ibid.

In 2015, the Ford Motor Company collected consumer data through their Ford vehicles' sensors, remote app-management software, and voice recognition system. Then, the company analyzed the collected consumer data and improved their noise reduction technology after realizing that "surrounding noise affected the performance of the software."[70] Ford demonstrates potential within traditional manufacturing industries, like the automotive one, for advancements in innovation based on data collection, especially with the increasing number of sensors on vehicles;[71] BMW, a German motor company, also uses big data to detect issues and vulnerabilities before the release of their new models.[72] Another example of innovation in the e-commerce and transportation industry is transportation network company, Uber, whose services include ride-hailing and food delivery. Uber's business model functions on what American sociologist Amitai Etzioni coined as a "trust in strangers";[73] Uber drivers are essentially strangers who service consumers, who are also strangers. Opposing researcher Glen Whelan argues, "...platforms like Uber work, not because of their ability to foster trust between strangers…, but because of an underlying knowledge that their actions are observed," not dissimilar to the way that the Panopticon works.[74] Uber shows businesses *are* the innovators and thrive on the collection of user data, whether it be through tracking user locations or targeting food advertisements to consumers so they are enticed to utilize Uber Eats, the food delivery service.

---

[70] Niebel, Rasel, Viete, "BIG data—BIG gains?" 297.

[71] Ibid.

[72] Nir Kshetri, "Big data's impact on privacy, security and consumer welfare," *Telecommunications Policy* 38, no. 11 (December 2014): 1137. https://doi.org/10.1016/j.telpol.2014.10.002.

[73] Glen Whelan, "Trust in Surveillance: A Reply to Etzioni," *Journal of Business Ethics* 156, no. 4 (April 2019): 15. https://doi.org/10.1007/s10551-018-3779-4.

[74] Jane Andrew and Max Baker, "The General Data Protection Regulation in the Age of Surveillance Capitalism," *Journal of Business Ethics* 168, no. 3 (January 2021): 569. https://doi.org/10.1007/s10551-019-04239-z.

With the aforementioned contact tracing situation in South Korea, big data has been known to aid the minimization of communicable diseases spreading. During Haiti's 2010 cholera outbreak, the disease could have been detected two weeks in advance if health officials were given data mined from Twitter and online news reports.[75] Moving from general health benefits to the health care sector, big data can be used to "identify drug interactions and design improved drug therapies"[76] as well as enforcing "effective drug regulation and reduc[ing] direct costs of medical expenditures and indirect costs associated with lower productivity"[77] through the collection of patient data. Dr. Kyu Rhee, chief medical officer of Aetna at CVS Health, commented on the advances of IBM Watson, a computer system that can quickly interpret information: "What we have done with Watson is we have applied it to medical and to health care. It has learned medical literature, it understands a medical record and can understand a medical image that a cardiologist may use, whether it is an MRI or a CT scan."[78] With Watson, the time to clear junk data, process proper data, and interpret medical data has been greatly reduced, especially regarding translating DNA material, genetic profiles, and personal treatment options.[79] As a result, those in the medical sector are optimistic about the use of patient data under the scope of big data; health care workers do not view big data technology as replacements, but rather supplements to their field.

[75] Kshetri, "Big data's impact," 1136.
[76] Niebel, Rasel, Viete, "BIG data—BIG gains?" 297.
[77] Kshetri, "Big data's impact," 1137.
[78] Josephine McKenna, "Big data:big promise," *European Heart Journal* 38, no. 7 (February 14, 2017): 470. https://doi-org.ezproxy.bu.edu/10.1093/eurheartj/ehx021.
[79] Ibid.

## Criticisms Attacking Zuboff

Zuboff continually remarks on the negatives associated with surveillance capitalism, but clearly there are many benefits to it as well, as this report has previously shown. Thus, it is important to exercise caution towards Zuboff's arguments and understand the critiques of her works. One way Zuboff describes surveillance capitalism is as, "a new economic order that claims human experience as a free source of raw material."[80] According to Zuboff, surveillance capitalism is primarily connected to companies like Facebook and Google, who analyze consumer behavior and sell it to advertisers for a profit. In contrast, technology and national security journalist Jacob Silverman argues that Zuboff should emphasize the importance of deregulation in surveillance capitalism. Silverman believes that the declining power of labor is beneficial to surveillance capitalism and argues that Zuboff's book *The Age of Surveillance Capitalism* does not have the most "straightforward beliefs"; instead, the book supports opinions that are in the minority.[81]

Moreover, Blayne Haggart, yet another critic of Zuboff, defines the differences between academic and polemic writing, arguing Zuboff's book cannot be held to the same academic standards as other authors in the field of surveillance capitalism. In his post, Haggart outlines Zuboff's "four tells of poor academic scholarship" in *The Age of Surveillance Capitalism*. First, Zuboff "exaggerated claims to novelty," claiming she coined the term 'surveillance capitalism,' but failed to mention her peers in the field like Nick Srnicek, whose book tackles a similar topic as hers. Second, Zuboff has an "absence of relevant literature" and fails to provide the proper

[80] Zuboff, *The Age of Surveillance Capitalism*.
[81] Silverman, "How Tech Companies Manipulate."

sources to refute her claims; instead, Zuboff cherry-picks sources that support her claims.[82] Third, Haggart claims that Zuboff has an "unclear framework [and thesis]" in her book. Zuboff presents what appears to be a singular thesis on surveillance capitalism. However, Haggart argues that it actually encompasses two underlying theses that she is unaware of: behavior modification and data extraction. These two theses lead to a change in the economic order.[83] Fourth, Zuboff often uses hyperboles in the text; Haggart states that Zuboff's "...argument stops relying so much on reason, logic and evidence – the foundation of an academic's authority – and begins relying on how it makes the reader feel."[84] In other words, Zuboff must rely on appealing to the reader's emotions as a persuasion tactic since her claims are weak. Haggart concludes Zuboff opts for polemic writing, which undermines her claims about surveillance capitalism.

[82] Blayne Haggart, "Evaluating scholarship, or why I won't be teaching Shoshana Zuboff's The Age of Surveillance Capitalism," *Orangespace*, February 15, 2019. https://blaynehaggart.com/2019/02/15/evaluating-scholarship-or-why-i-wont-be-teaching-shoshana-zuboffs-the-age-of-surveillance-capitalism/

[83] Ibid.

[84] Ibid.

## Drawbacks to Surveillance Capitalism

### Facebook, Cambridge Analytica, and Elections Issues

In March 2018, articles were published revealing elements of the scandal that would soon follow Cambridge Analytica, a data firm that documented to have improperly used Facebook's data to "build voter profiles." Sparking federal investigation and sending Facebook into its biggest crisis yet, Cambridge Analytica collected millions of Facebook users' information in 2015 without the users knowing.[85] In 2018, Facebook admitted to mishandling over 50 million of its users' data that was improperly obtained by Cambridge Analytica. Months later, the number rose to 87 million impacted Facebook users.[86] In March 2018, Cambridge Analytica's whistleblower employee, Christopher Wylie, came forward and revealed the extent of the data firm's activities to *The New York Times* and *The Guardian.* Consequently, Facebook issued an apology and Facebook's CEO, Mark Zuckerberg, swore an oath in front of Congress, while the FTC issued Facebook a historic fine to the tune of $5 billion.[87]

The question becomes, how was the data obtained in the first place? The data was obtained through a personality quiz, "thisisyourdigitallife," that paid 270,000 people to take it. The quiz, developed by Aleksandr Kogan, a Russian Psychology professor at the University of Cambridge, "who shared the information in a commercial partnership with Strategic Communication Laboratories (SCL), which later created Cambridge Analytica" also gathered data from not only the users who took the quiz themselves, but also from the users' friends, who

[85] Silverman, "How Tech Companies Manipulate."

[86] Alexandra Ma and Ben Gilbert, "Cambridge Analytica: a Guide to the Trump Linked Data Firm That Harvested 50 Million Facebook Profiles," *Business Insider*, accessed August 23, 2019, https://www.businessinsider.com/cambridge-analytica-a-guide-to-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-2018-3.

[87] Ibid.

were unaware of their data being taken. This resulted in the vast stash of data from 87 million users, most of whom were from the US[88] Cambridge Analytica amassed personal information including details about where users lived and what pages they liked, which in turn, enabled them to create psychological profiles that "analyzed characteristics and personality traits." The Cambridge Analytica Quiz was part of a larger Qualtrics (an online survey management company) psychology questionnaire. Those who filled out the questionnaire first had to grant access to their Facebook profiles, and once they granted access, an app harvested their and their friends' data.[89]

Cambridge Analytica's data collection is alarming because the same information was later deployed in political campaigns, enabling Cambridge Analytica to target users through their psychological profiles and encourage them to vote for presidential candidates in the 2016 presidential election. Wylie explained, "We exploited Facebook to harvest millions of people's profiles. And built models to exploit what we knew about them and target their inner demons."[90] In 2016, the Trump campaign hired Cambridge Analytica, to use voter data gathered from millions of Americans to target ads towards them.[91] This is not the first instance of collaboration with high-level US Republicans in government, as Cambridge Analytica is owned by right-wing donor, Robert Mercer, and the company has worked with Texas Senator Ted Cruz in the 2016 Presidential Elections and has support from many Republicans. Additionally, Cambridge Analytica had ties to other high-level Republicans. Steve Bannon, Trump's White House Chief Strategist for the first seven months of his presidency, served on Cambridge Analytica's board.[92]

[88] Silverman, "How Tech Companies Manipulate."
[89] Ibid.
[90] Ibid.
[91] Ma and Gilbert, "Cambridge Analytica."
[92] Lyon, "Surveillance Capitalism," 74.

Cambridge Analytica suspended its Chief Executive, Alexander Nix, after a British channel released an undercover video in which he suggested the company had used bribery and seduction to influence foreign elections and entrap politicians.[93] *The Observer* and *The Times* have reported allegations that 2016's 'Brexit' campaign utilized a Cambridge Analytica contractor to help go around election spending limits and implicated two senior advisors to Former Prime Minister Theresa May. Wylie further supported that Cambridge Analytica helped Brexit gain favorable public opinion, which aided in Britain's dissolvement from the EU[94]

Users were outraged by these shocking revelations and subsequently became interested in Facebook's controversial protection of users' privacy.[95] Soon after the Cambridge Analytica issues were publicized, users began to generate a "#deletefacebook," and many sought to delete themselves from the platform, especially in the UK and Canada.[96]

## The 1st and 4th Amendments of the United States Constitution

On December 2, 2015, a terrorist attack occurred at the Inland Regional Center in San Bernardino, California. The FBI recovered an Apple iPhone which belonged to one of the perpetrators of the attack, Syed Rizwan Farook. Unable to unlock the phone's four digit passcode, the FBI turned to Apple to create a new version of the phone's iOS operating system that could be installed and disable certain security features iOS devices contain as Apple phones are programmed to automatically delete all data after ten failed password attempts.[97] Apple

[93] Silverman, "How Tech Companies Manipulate."
[94] Ibid.
[95] Ibid.
[96] Lyon, "Surveillance Capitalism."
[97] Saeed Ahmed and Ralph Ellis, "Mass Shooting at Inland Regional Center: What We Know," *CNN*, December 5, 2015. https://www.cnn.com/2015/12/03/us/what-we-know-san-bernardino-mass-shooting.

declined the FBI's request and their chief executive, Tim Cook, issued a statement in which he said, "The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers… we oppose this order, which has implications far beyond the legal case at hand."[98] Apple and other top tech companies such as Google and Facebook made the case that the court order threatened the privacy of individuals. As a result, Apple Inc. filed a 65-page legal response to the court order stating that they should unlock Syed Farook's phone for the FBI. Lisa Olle, Apple's manager for global privacy and law enforcement responded and explained that "if a purpose built operating system such as the one the government seeks here got into the wrong hands it would open a significant new avenue of attack, undermining the security protections that Apple spent years developing to protect its customers."[99] Apple's motive for opposing the court order lies in the fact that the request made by the FBI threatened data security by establishing a precedent that the US government could use to mandate any technological company to create a software that could undermine the security of their products. The court order against the company required Apple to write code, violating the US Constitution's first amendment right to freedom of speech, as computer code has legally been labelled as protected speech.[100]

Furthermore, the Constitution and the nation's laws limit how investigators and prosecutors can collect evidence. In a 1977 case involving the New York Telephone Company, the Supreme Court stated the government could not compel a third party that is not involved in a

[98] "Why Apple Is Right to Challenge an Order to Help the F.B.I," *The New York Times*, February 19, 2016. https://www.nytimes.com/2016/02/19/opinion/why-apple-is-right-to-challenge-an-order-to-help-the-fbi.html.

[99] Matt Burgess, "Why Apple Won't Unlock IPhones for the FBI," *WIRED UK*, February 26, 2016. https://www.wired.co.uk/article/why-apple-refuse-help-fbi-iphone.

[100] Mitchell Nemeth, "Will Privacy Continue to Take a Backseat to Surveillance Capitalism," *Medium*, January 25, 2020. https://towardsdatascience.com/will-privacy-continue-to-take-a-backseat-to-surveillance-capitalism-9cd6fc6b597c.

crime to assist law enforcement if doing so would place 'unreasonable burdens' on it.[101] Cook expressed that the court order requiring Apple to create software to subvert the security features of an iPhone places just such a burden on the company. He further communicated concern regarding that writing a new code would have an effect beyond unlocking one phone.[102] If Apple were to help the FBI in this case, courts could potentially use this software in future investigations or order it to create new software to fit new needs. Additionally, the nation's fourth amendment could be compromised as hackers may be able to pilfer software from company servers. Many technological companies are able to maintain access to or create a backdoor to encrypted data on electronic devices which can cause further harm as criminals and domestic and foreign intelligence agencies are able to manipulate such features to conduct mass surveillance. [103]

## Cyberwarfare, Hacking, and the Dark Web Market

On July 29, 2017, Equifax — a data broker company whose product is "aggregated consumer information collected from third parties and dragnet surveillance initiatives" — had been compromised, affecting 143 million Americans' credit records and about 200,000 consumers' credit card information.[104] It was discovered that Equifax was being exploited for at least two months, but none of this information was publicized until September 7, 2017.[105]

---

[101] *United States V. New York Telephone Co., 434 U.S. 159 (1977)*, (n.d), https://supreme.justia.com/cases/federal/us/434/159/.

[102] "Why Apple Is Right to Challenge an Order to Help the F.B.I."

[103] Nemeth, "Will Privacy Continue."

[104] James Scott, "Equifax: The Hazards of Dragnet Surveillance Capitalism," *Institute for Critical Infrastructure Technology*, (October 2017): 4. https://icitech.org/wp-content/uploads/2017/10/ICIT-Analysis-Equifax-The-Hazards-of-Dragnet-Surveillance-Capitalism.pdf.

[105] Ibid, 6.

Equifax's data included consumers' extremely sensitive information, including social security numbers and purchasing habits, which became available once breached. Senior Fellow and cybersecurity researcher James Scott noted: "Now, the attacker(s) can also make predictions and assessments of consumers' lives, in addition to compromising financial accounts and stealing identities."[106] This data breach highlighted two issues: the data economy outgrew consumer protections and there was an apparent lack of transparency on data breaches. Scott criticized the lack of congressional legislation on the breaching matter and suggested that "those [Equifax] individuals, who profited for years on consumer data, should be held criminally negligent for their failure to protect it according to its value."[107] By not holding these data broker companies accountable for the security of personal data, which these businesses profit on, justice and peace cannot be served to those who suffer on behalf of the breaches. Although Equifax is one example of a data breach, it has been reported that 235 million social media profiles were *accidentally* made available by Hong Kong-based security firm Social Data due to negligence of 'web-scraping,' when a company scrapes data from sites or apps to collect in a database and use it to approach individual users.[108] The situation is worse because consumers are passive in the data market — consumers do not have proper control over their own data.

The Equifax data breach gives insight into the purpose of cybercrime: it is cheap, effective, and anonymous. Lurking in the cyberspace and data economy is a place known as the 'Dark Web,' which is like the Internet (clearnet) but the web traffic is anonymized, meaning the buyers, sellers, and anyone browsing the 'Dark Web' remain anonymous. Blogger Dan Patterson

---

[106] Scott, "Equifax," 5-6.
[107] Ibid, 14.
[108] Mike Fong, "The lurking security risks of surveillance capitalism," *Security Magazine*, November 5, 2020. https://www.securitymagazine.com/articles/93835-the-lurking-security-risks-of-surveillance-capitalism.

launched his own investigation into the 'Dark Web,' discovering that sensitive information such as social security numbers and addresses could be bought at the low price of $69. Further into his investigation, Patterson surprisingly discovered his own sensitive information was available in the dark web market.[109] Here is where the leaked and hacked data are sold — Patterson bluntly states the 'Dark Web' affects every Internet user and "[i]f your data was leaked as part of a government or corporate hack, it's for sale on the Dark Web."[110] The previously mentioned benefits for the health care sector becomes minimized — all sensitive patient data can easily be hacked and put for sale on the 'Dark Web.' In fact, the health care sector has always been at risk of becoming the most breached sector due to its amount of sensitive data, but lack of high security standards.[111] Cybercrime is a booming business since anyone can be a hacker. The profit cycle is simple: for every successful hack or breach, the attacker earns money, then the perpetrator has more capital to use for the next set of attacks.[112] Because the profit cycle is so simple, other competitors want to capitalize on the gains through the 'Dark Web' too. Thus begins the vicious cycle of corruption involving personal data, the 'Dark Web,' and anonymous hacking.

Surveillance capitalism has created a climate in which underground activity is encouraged — the underbelly of the data economy. Because of the commodification and

---

[109] Curtis Buhrkuh, "Horror Stories from the Dark Web," *Office1*, November 3, 2020. https://www.office1.com/blog/horror-stories-from-the-dark-web.

[110] Dan Patterson, "Dark Web: A cheat sheet for business professionals," *TechRepublic*, October 26, 2018. https://www.techrepublic.com/article/dark-web-the-smart-persons-guide/.

[111] Steve Andriole, "Cyberwarfare Will Explode in 2020 (Because It's Cheap, Easy And Effective)," *Forbes*, January 14, 2020. https://www.forbes.com/sites/steveandriole/2020/01/14/cyberwarfare-will-explode-in-2020-because-its-cheap-easy--effective/?sh=4f1e1f986781.

[112] Daniel Schiappa, "The Big Business of Cybercrime: The Dark Web," *Forbes*, September 12, 2019. https://www.forbes.com/sites/forbestechcouncil/2019/09/12/the-big-business-of-cybercrime-the-dark-web/?sh=61cdd9a15142.

increased value of collecting personal information and data, there are some players in the data market competing for the valuable resource through illegal means. After US President Trump's decisions to withdraw from the Iran nuclear deal and provoking trade disputes with China during his term, there was increased espionage and hacking on American citizens' data and intellectual property.[113] The fear of Chinese hacking for American data further fueled Trump's push on allies to ban Huawei, a Chinese technology company, from their 5G network build-out.[114] In December 2020, it was discovered that 9 federal agencies and 100 private sector companies were compromised by the Russian-backed SolarWinds hack, a major cyberattack which led to a series of data breaches and a hacking campaign which was believed to have started in late 2019 or early 2020.[115] The Council on Foreign Relations has a "Cyber Operations Tracker" which is a database of publicly known state-sponsored incidents that have occurred worldwide since 2005 and it notes: "China, Russia, Iran, and North Korea sponsored 77 percent of all suspected operations. In 2019, there were a total of seventy-six operations, most being acts of espionage." The number of cyber operations support this: China leads with 153, Russia with 93, Iran with 53, and North Korea with 36. In the western hemisphere, the total number of cyber operations totals to 18: 15 for America, 1 for Canada, 1 for Mexico, and 1 for Panama [See Appendix C].[116] Governments are involved with cyber warfare because they are aware of data's high value. Once they attain personal data, it can be converted to behavioral data, then from there, power is endless. As

---

[113] Robert Hackett, "Cyber Saturday—Rise of 'Surveillance Capitalism,' China and Iran Go Hacking, Facebook as 'Digital Gangster'," *Fortune*, February 23, 2019. https://fortune.com/2019/02/23/surveillance-capitalism-book-facebook-gangster-china-iran-hacking/.

[114] Ibid.

[115] Robert K. Knake, "Why the SolarWinds Hack is a Wake-Up Call," *Council on Foreign Relations*, March 9, 2021. https://www.cfr.org/article/why-solarwinds-hack-wake-call.

[116] "Cyber Operations Tracker," *Council on Foreign Relations*, accessed April 21, 2021. https://microsites-live-backend.cfr.org/cyber-operations.

mentioned previously, control over behavioral data has led to interference with sensitive matters such as elections which, in turn, influences countries, its people, its politics, and its history.

Cyber warfare has been deemed evitable because of government reluctance to self-police.[117] According to *Wired Magazine* writer Andy Greenberg, governments are unwilling to deal with cyber threats "because they don't want to limit their own freedom to launch cyberattacks at their enemies…," including the US[118] Paranoia surrounding hacking has a valid basis — many cybersecurity firms and virtual private network service providers have predicted that cyberattacks will skyrocket in the following years. With technological advancements come technological vulnerabilities which have yet to be considered since technological developments are produced quicker than can be fully assessed of its weaknesses; hacking advancements are also being made, which leaves the outdated technologies vulnerable. Many examples occur today: the hacking of SIM cards, text messages, and calls; mobile payment and phishing scams; 'deepfakes' (a normal person's face on a video can be virtually be replaced by a well-known person) spreading fake news; and malware attacks.[119] The list expands further; it is concerning that the list of blackhat hacking tactics outweigh the options for personal data security. The dangerous environment which surveillance capitalism fosters — one in which practices to get personal data cheaper, quicker, and more secretly will be more profitable — reveals the necessity for governmental regulation to combat these issues.

[117] Andriole, "Cyberwarfare Will Explode in 2020."
[118] Ibid.
[119] Ibid.

## Legislation Challenges

### Ethical Implications and Complications

The first, and most obvious, of the ethical complications that come up in surveillance capitalism are the general concerns relating to consumers' privacy. Companies are mining users for data ruthlessly just to make more money, and it is often done without the knowledge of consumers; clearly, ethics is not a primary area of concern for companies. Additionally, this brings up the issue of ownership and personal and/or private property regarding data. Do we own our own data? If not, who does, if anyone at all? Would it be considered stealing if corporations are taking data without the consent of the consumer, or even if the consumer is not aware of that they are?[120]

Beyond that, corporations are not just seeking to collect data to use to target and optimize advertisements and such, they are also seeking to influence consumer behavior. With this in mind, it may be relevant to ask whether Foucault's theory of *panopticism* is actually more relevant today under surveillance capitalism than later theorists like Deleuze, Haggerty, or Ericson acknowledged — possibly because it *was* less relevant in the earlier 2000s, when the Internet was not quite as prevalent as it is today. Behavior modification is characteristic of the 'discipline' that Foucault emphasizes when discussing his version of the Panopticon.[121] Haggerty and Ericson particularly strayed from severe and explicit condemnation of society and modern surveillance because it was *not* like the older panoptical and disciplinary forms.[122] If under surveillance capitalism, surveillance is becoming more internalized by corporations, how much

[120] Evan Malmgren, "Resisting 'Big Other': What Will It Take to Defeat Surveillance Capitalism?" *New Labour Forum* 28, no. 3 (2019): 42-50. https://journals.sagepub.com/doi/10.1177/1095796019864097.
[121] Galič, Timan, and Koops, "Bentham, Deleuze and Beyond."
[122] Haggerty and Ericson, "The surveillant assemblage."

more of an ethical disaster is this situation? Without regulation, corporations would make use of both 'discipline' *and* 'control' when surveilling consumers, a new and almost definitely lethal amalgam that is distinctive of surveillance capitalism.

Especially regarding the large amount of personal and intimate data that corporations collect about users, another relevant question arises: how different is the Deleuzean concept of the *dividual* in surveillance capitalism really from the actual individual themselves? What happens when every possible piece of information about a person is "relevant data" for companies? The 'data-doubles,' as have been addressed previously, are meant to be superficial pockets of data about a person that are most relevant to companies in order to make a profit.[123] However, companies know information about us specifically, our deep thoughts, feelings, and desires and to be able to predict our actions.[124] It is as if they are able to peer into our unconscious and extract information about ourselves that we could not possibly be able to give our consent to. Besides the evident ethical issues that arise simply from data extraction, what will corporations do with such personal and intimate data? It could potentially be harmful in a myriad of different ways, especially if put into the wrong hands — and with profit being the goal, it is more than likely that this data would be. The point is not to paint a dystopian vision of big data and surveillance capitalism gone wild, but more so to emphasize the pressing need for regulation in an industry where ethics holds very little weight.

The last ethical issue is the power imbalance between consumers and corporations. Companies are in a position of power where they are able to take our data — our 'surplus information' — and sell it, while leaving the consumer almost entirely out of the exchange. So

[123] Galič, Timan, and Koops, "Bentham, Deleuze and Beyond."
[124] Wake, "3 Ways That Social Media Knows."

long as consumers are not given a seat at the table in having the power to control their own data, this relationship will always be unequal. While signing a "Terms of Agreement" might seem fair, holding both parties accountable on equal grounds, it really is unfair because this social contract is not mutually agreed upon by equal parties. The corporation has the advantage and the consumer must agree to the contract to use the services of the company, which many people in society have become so dependent on. It is unethical for a corporation to continue to play into this power imbalance and to not allow the consumer total power over their own data.[125]

Thus, the regulatory solution to this issue particular to surveillance capitalism must be one that involves restoring this power to the consumer. There can be, and needs to be, some kind of regulation which will prevent the exploitation of the consumer by the corporation. Lastly, it is important to note that while big data *can* be used harmfully, it does not *have* to be, as we have previously discussed with things like contact tracing and the advances that have been made in the medical field particularly.

**Ambiguity, Confusion, and Unknowingness**

Surveillance capitalism thrives in cyberspace, an area that has been difficult to regulate. Organizations like the UN, WTO, and WHO are international regulation bodies that govern peace, trade, and health. Yet, for big data and surveillance capitalism, there is no international regulation body even when the transaction of personal data occurs on a worldwide basis. The ambiguity of which field surveillance capitalism fits under confuses which body should regulate

[125] Jonathan Cinnamon, "Social Injustice in Surveillance Capitalism," *Surveillance & Society* 15, no. 5 (2017): 609-625. https://search-proquest-com.ezproxy.bu.edu/docview/1991088392?pq-origsite=primo&accountid=9676.

it. Is it a data issue? An economic issue? An international crime issue? Even if this issue can be cleared up through domestic legislation, another concern with regulating big data and surveillance capitalism within cyberspace is the anonymity of anyone in the data market. In the case of hackers, how can anonymous, difficult-to-trace perpetrators be held accountable if their identities are unknown? How can unknown attackers be punished?

Even then, if *those* issues are cleared up, how does one regulate the data collectors (governments and companies) who hold a clear monopoly on user data? Current US legislation does not hold the collectors who have been breached or have recklessly released data accountable for their actions. The reason for lack of legislation enforcement on the big data monopoly is the illiteracy of big data within the public sector. As the development of new data technologies increases, senior officials within the US government have to keep up with the advancements. Through the Senate testimony on Cambridge Analytica in 2018, the "grilling" of Mark Zuckerberg, CEO of Facebook, has proven how outdated US government officials are on social media platforms, data, and technology issues. Utah Senator Orrin Hatch asked Zuckerberg how Facebook earns money through its free social media platform, in which Zuckerberg bluntly replied, "Senator, we run ads."[126] Florida Senator Bill Nelson asked about the option to avoid advertisements about chocolate, to which Zuckerberg responded that "targeted ads are simply a part of Facebook's user agreement and are commonplace in general on the Internet."[127] Mississippi Senator Roger Wicker asked if Facebook could track user browsing history when logged out of the site and Zuckerberg had to explain how the idea of 'cookies,' a computer

[126] Summer Meza, "Zuckerberg spent an absurd amount of time explaining how the internet works in his Senate testimony," *The Week*, April 10, 2018. https://theweek.com/speedreads/766564/zuckerberg-spent-absurd-amount-time-explaining-how-internet-works-senate-testimony.

[127] Ibid.

identifier, functions.[128] Even further in the testimony, Zuckerberg was able to maneuver the questions due to the senators' lack of knowledge on how social media, data, and, frankly, the Internet works.[129] How can legislation be established if those in charge of creating it cannot understand the basic functions of the Internet, the very cyberspace in which surveillance capitalism exists? In fairness, if senators cannot understand this concept, then how can we place that same responsibility on consumers to understand this concept of big data and surveillance capitalism? There is an epistemological power imbalance between corporations and basically everyone else so it is essential that both citizens and the public sector keep up with the information on big data. A general proposition would be to impose education on big data to increase digital civic literacy on the matter, especially at the K-12 level, but implementing this into school curricula would have to develop over an unspecified period of time.

[128] Meza, "Zuckerberg spent an absurd amount."

[129] Shara Tibken, "Questions to Mark Zuckerberg show many senators don't get Facebook," *CNET*, April 11, 2018. https://theweek.com/speedreads/766564/zuckerberg-spent-absurd-amount-time-explaining-how-internet-works-senate-testimony.

## The European Union's General Data Protection Regulation

In 2018, the European Union put the General Data Protection Regulation (GDPR) into effect.[130] The law requires companies to have protocols that will protect the privacy and personal information of citizens within the EU. This law is considered to be one of the most severe laws regarding data/cyber security around the world. Although it was created by the European Union, the legislation is also required to be applied to other international organizations that might be targeting any citizens within the countries in the European Union., Those who violate the law will receive fines and penalties.[131] This regulation is a sign of the European Union's attitude towards data privacy and security during the digital revolution.

There are different parts to the regulation. For data security, companies are required to deal with data by utilizing any technical or organizational measures. An example of a technical measure is utilizing two-factor authentication, such as Duo Security, on accounts containing any personal information. An example of an organizational measure is including a section of data privacy in the employee handbook or "limiting access to personal data to only those employees"[132] who need it. Additionally, if a company faces a data breach, they have up to three days to notify their employees before they face any fines. For data protection, every organization has to recognize every creation "by design and by default."[133] Essentially, everytime an organization creates a product or service, they have to consider the personal data aspect of the app.

---

[130] Ben Wolfard, "What is GDPR, the EU's new data protection law?" *GDPR EU*, Accessed April 23, 2021. https://gdpr.eu/what-is-gdpr/

[131] Ibid.

[132] Ibid.

[133] Ibid.

Article 6 of the legislation details scenarios of when companies are legally allowed to process a person's information. Companies have to make sure that specific people have given clear consent for companies to utilize that data as they have "opted-in" to the company's services. Companies can access this information when they are preparing a contract where one's information has to be analyzed, such as doing a background check for a job. However, the scenario that is constantly evolving is when a company expresses interest to process one's personal information. But, one's "fundamental rights and freedoms of the data subject"[134] always trumps a company's interest.

[134] Wolfard, "What is GDPR."

## Policy Recommendation

### Proposal

The main issues in the US include the three "lacks": lack of reciprocity between collectors and users, lack of user control over personal data, and lack of big data knowledge for the public. These issues have led to a collector monopoly on data, behavior modification, and lack of legislation regarding the security of personal data privacy. Tackling the lack of user control over personal data will solve the subsequent issues. As the NECDP, the knowledgeable body of policymakers on big data and surveillance capitalism, we have the credibility to establish our proposed American Privacy Protection Act (APPA).

In the past, lawmakers have proposed self-regulation as the most viable option. The US Children's Online Privacy Protection Act (COPPA) monitors the privacy and security of data of children, but researchers discovered many apps violate COPPA, suggesting "it is not clear that industry self-regulation has resulted in higher privacy standards; some of our data suggest the opposite."[135] Based on the information, it has shown that self-regulation is ineffective in surveilling the collection of big data. Instead, the FTC will work to regulate the collection of big data because it has authority to protect consumer protection in all industries. The FTC "enforces federal consumer protection laws"; "promotes competition"; and protects consumers through halting fraudulent, deceptive, and unfair marketplace activities.[136] The most effective option is to expand the FTC's power through the Customer Online Notification for Stopping Edge-provider

[135] Donell Holloway, "Surveillance capitalism and children's data: the Internet of toys and things for children," *Media International Australia* 170, no. 1 (February 2019): 29. https://doi.org/10.1177/1329878X19828205.

[136] "What We Do," *Federal Trade Commission*, accessed April 20, 2021. https://www.ftc.gov/about-ftc/what-we-do.

Network Transgressions (CONSENT Act) and increase user control over their data through the Social Media Privacy Protection and Consumer Rights Act (SMPPCR Act).

The first necessary step is to expand the FTC's authority because its powers are quite limited; the FTC currently "has little to no oversight over a range of businesses and industries."[137] The CONSENT Act was first proposed in the Senate by Massachusetts Senator Ed Markey in 2018. The bill would "[direct] the [FTC] to establish privacy protections for customers of online edge providers (e.g., search engines, streaming services, and social-media platforms)" by requiring providers to "notify customers about [their data]; obtain opt-in consent to use, share or sell [their data]; develop certain data-security practices; and notify customers in the event of a security breach."[138] Because the bill relies on the FTC to enforce any violations of its intended rules, the passing of the bill would force the FTC's power to expand.[139] Then, the FTC will be able to effectively implement the second part of the proposal.

The second necessary step is to pass the APPA through Congress. The APPA is an American law that specializes in data protection and privacy, inspired by the EU's GDPR. The US and EU trade relations have proven to be one of the strongest in the world. In 2018 alone, the US exported $218 billion to the EU and the EU exported $127 billion to the US.[140] However, the passing of the GDPR in the EU has proven to be detrimental to the US. As previously

---

[137] Derek Hawkins, "The Cybersecurity 202: Why a privacy law like GDPR would be a tough sell in the U.S.," *The Washington Post*, May 25, 2018. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/25/the-cybersecurity-202-why-a-privacy-law-like-gdpr-would-be-a-tough-sell-in-the-u-s/5b07038b1b326b492dd07e83/.

[138] U.S. Congress, Senate, Committee on Commerce, Science, and Transportation, *Consumer Online Notification for Stopping Edge-provider Network Transgressions or the CONSENT Act: Summary (to Accompany S.2639)*, 115th Cong., 2d sess., 2018, S. Doc., https://www.congress.gov/115/bills/s2639/BILLS-115s2639is.pdf.

[139] Russell Brandom, "After Facebook hearing, senators roll out new bill restraining online data use," *The Verge*, April 10, 2018. https://www.theverge.com/2018/4/10/17221046/facebook-data-consent-act-privacy-bill-markey-blumenthal.

[140] "EU Data Protection Rules and U.S. Implications," *Congressional Research Service*, July 17, 2020. https://fas.org/sgp/crs/row/IF10896.pdf

mentioned, the GDPR is the EU's data privacy law that requires organizations to protect individuals' personal data while simultaneously providing individuals with more control over their data. One of the major clauses of the GDPR is that it also applies to any international organization, regardless if they are EU-based.[141] Because the EU believes the regulation of privacy in the US is too lenient, businesses located in the EU are hesitant to work with the US due to the prevalence of self-regulation in the country.

In 2020, the state of California passed the CCPA. This holds significance to the economy because California has been credited with the fifth largest economy in terms of GDP.[142] Similarly to the EU's GDPR, the CCPA grants residents power to control and protect their privacy rights from organizations. The CCPA and GDPR share three main similarities: the ability to have access, information, and portability in the hands of the consumer. The CCPA has a similar clause to the GDPR where the legislation applies to any company that does business with California residents. However, other states are also beginning to introduce similar privacy legislation. Because all fifty states have different state laws, companies that function in multiple states may come across various standards which may cause issues in the future.[143]

The final step is to utilize the FTC's expanded authority to enact the APPA. We, the NECDP, propose a policy where the FTC will regulate and promote the APPA at the US federal level. After seeing California implement this legislation at a state level, we believe that this legislation could work at the federal level as well. Since it is constitutional at the state level, it is

---

[141] "EU Data Protection Rules."

[142] Caitlin Chin, "Highlights: The GDPR and CCPA as benchmarks for federal privacy legislation," *Brookings*, December 19, 2019. https://www.brookings.edu/blog/techtank/2019/12/19/highlights-the-gdpr-and-ccpa-as-benchmarks-for-federal-privacy-legislation/

[143] Ibid.

constitutional at the federal level. The FTC will monitor the implementation of our proposed APPA so that it does not violate the Fourth Amendment (the right to privacy). By implementing a similar model to the GDPR on the federal level, it would also benefit companies because by following an overarching federal privacy legislation, companies that operate in different states will not adhere to several state privacy legislations. Additionally, if the US regulates similarly to the GDPR privacy standards, trade relations would be stronger and smoother because of an established mutual trust. This would also incentivize the US to support and improve surveillance capitalism as there would be an increase in net exports, while protecting individuals' privacy rights.

We, the NECDP, believe that by implementing the American Privacy Protection Act, it will not only help the US economy and companies, but also protect and expand the privacy rights of our citizens.

# Appendices

## Appendix A

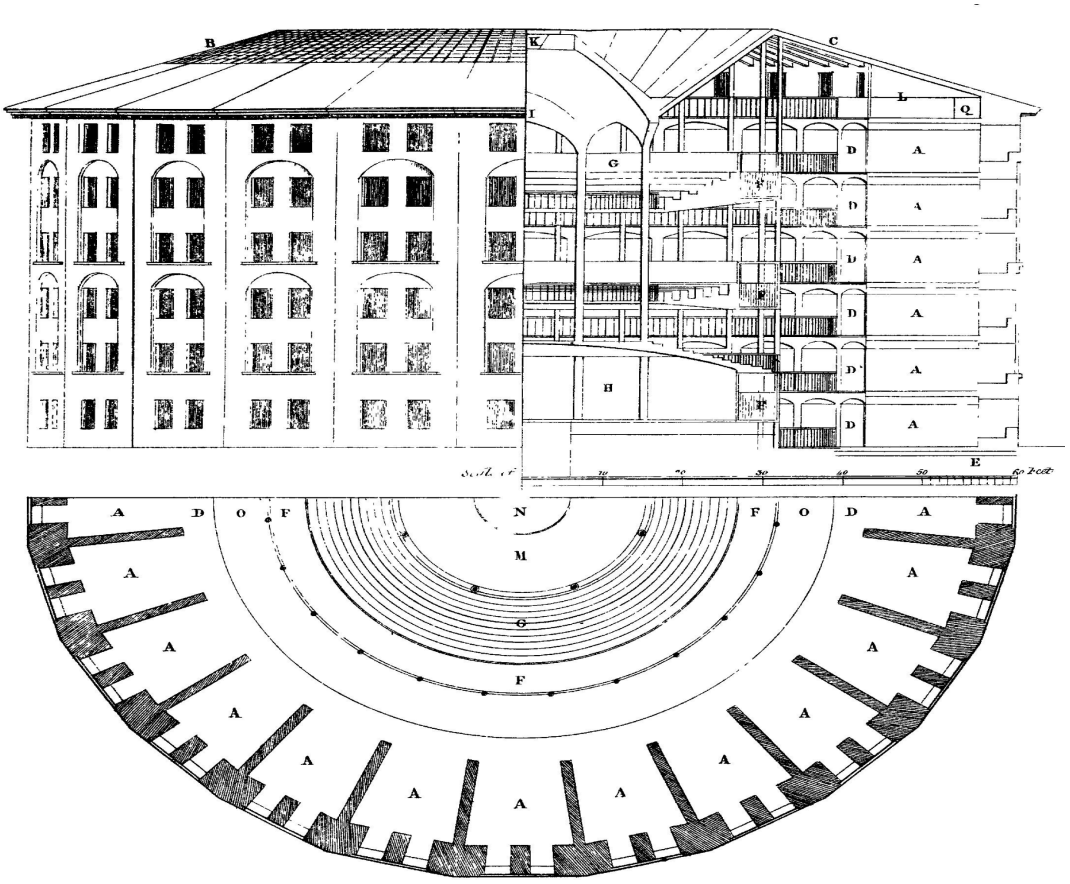



Diagram of Jeremy Bentham's prison-Panopticon. In the bottom part of the diagram, the circular space at the center is the watchtower where the inspector would observe the individuals.

Source: "Panopticon." *Wikipedia*, Wikimedia Foundation, March 31, 2021. en.wikipedia.org/wiki/Panopticon.

## Appendix B

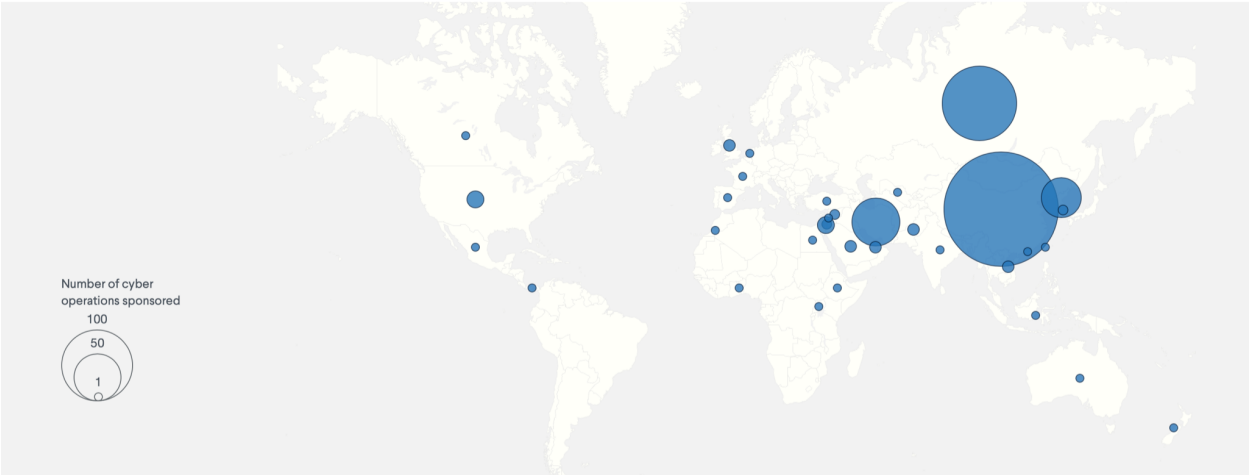
# Data Storage Units Chart: From Smallest to Largest

| Unit | Shortened | Capacity |
|---|---|---|
| Bit | b | 1 or 0 (on or off) |
| Byte | B | 8 bits |
| Kilobyte | KB | 1024 bytes |
| Megabyte | MB | 1024 kilobytes |
| Gigabyte | GB | 1024 megabytes |
| Terabyte | TB | 1024 gigabytes |
| Petabyte | PB | 1024 terabytes |
| Exabyte | EB | 1024 petabytes |
| Zettabyte | ZB | 1024 exabytes |
| Yottabyte | YB | 1024 zettabytes |

Chart of the units of data measurement from smallest to largest.

Source: Anna Birna Turner, "Data Storage Units of Measurement Chart from Smallest to Largest," *Solutions Review*, January 24, 2020. https://solutionsreview.com/data-storage/data-storage-units-of-measurement-chart-from-smallest-to-largest/.

## Appendix C




Visual of the amount of publicized cyber attacks since 2005 to its respective country.

Source: "Cyber Operations Tracker," *Council on Foreign Relations*, accessed April 21, 2021. https://microsites-live-backend.cfr.org/cyber-operations#Glossary.

**Bibliography**

"About the IAPP," *International Association of Privacy Professionals*, accessed April 22, 2021. https://iapp.org/about/what-is-privacy/.

Ahmed, Saeed, and Ralph Ellis. "Mass Shooting at Inland Regional Center: What We Know." *CNN*, December 5, 2015. https://www.cnn.com/2015/12/03/us/what-we-know-san-bernardino-mass-shooting.

Andriole, Steve. "Cyberwarfare Will Explode in 2020 (Because It's Cheap, Easy and Effective)." *Forbes*, January 14, 2020. https://www.forbes.com/sites/steveandriole/2020/01/14/cyberwarfare-will-explode-in-2020-because-its-cheap-easy--effective/?sh=4f1e1f986781.

"Facebook's Data-Sharing Deals Exposed." *BBC News*, December 19, 2018. https://www.bbc.com/news/technology-46618582.

Baca, George. "Eastern surveillance, Western malaise, and South Korea's COVID-19 response: oligarchic power in Hell Joseon." *Dialectical Anthropology* 44, (August 24, 2020): 301-307. https://doi.org/10.1007/s10624-020-09609-y.

Brandom, Russell. "After Facebook hearing, senators roll out new bill restraining online data." *The Verge*, April 10, 2018. https://www.theverge.com/2018/4/10/17221046/facebook-data-consent-act-privacy-bill-markey-blumenthal.

Breckenridge, Keith. "Capitalism without Surveillance?" Review of *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, by Shoshana Zuboff. *Development and Change* 51, no. 3 (May 19, 2020): 921-935. https://doi-org.ezproxy.bu.edu/10.1111/dech.12588.

Buhrkuh, Curtis. "Horror Stories from the Dark Web," *Office1*, November 3, 2020. https://www.office1.com/blog/horror-stories-from-the-dark-web.

Burgess, Matt. "Why Apple Won't Unlock IPhones for the FBI." *WIRED UK*, February 26, 2016. https://www.wired.co.uk/article/why-apple-refuse-help-fbi-iphone.

*California Consumer Privacy Act (CCPA)*. Office of the Attorney General, July 9, 2020. https://oag.ca.gov/privacy/ccpa.

Chin, Caitlin. "Highlights: The GDPR and CCPA as benchmarks for federal privacy legislation." *Brookings*, December 19, 2019.

https://www.brookings.edu/blog/techtank/2019/12/19/highlights-the-gdpr-and-ccpa-as-benchmarks-for-federal-privacy-legislation/

Cinnamon, Jonathan. "Social Injustice in Surveillance Capitalism." *Surveillance & Society* 15, no. 5 (2017): 609-625. https://search-proquest-com.ezproxy.bu.edu/docview/1991088392?pq-origsite=primo&accountid=9676.

Cornett, Kristen. "Companies tracking you on social media; How do they do it?" *Dayton 24/7*, November 2, 2018. https://dayton247now.com/news/local/companies-stalking-you-on-social-media-how-you-can-control-what-they-know-about-you.

"Cyber Operations Tracker." *Council on Foreign Relations*, accessed April 21, 2021. https://microsites-live-backend.cfr.org/cyber-operations.

"EU Data Protection Rules and U.S. Implications." *Congressional Research Service*, July 17, 2020. https://fas.org/sgp/crs/row/IF10896.pdf

Fong, Mike. "The lurking security risks of surveillance capitalism." *Security Magazine*, November 5, 2020. https://www.securitymagazine.com/articles/93835-the-lurking-security-risks-of-surveillance-capitalism.

Galič, Maša, Tjerk Timan, and Bert-Jaap Koops. "Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation." *Philosophy & Technology* 30, (2017): 9-37. https://doi.org/10.1007/s13347-016-0219-1.

Hackett, Robert. "Cyber Saturday—Rise of 'Surveillance Capitalism,' China and Iran Go Hacking, Facebook as 'Digital Gangster'." *Fortune*, February 23, 2019. https://fortune.com/2019/02/23/surveillance-capitalism-book-facebook-gangster-china-iran-hacking/.

Haggart, Blayne. "Evaluating scholarship, or why I won't be teaching Shoshana Zuboff's The Age of Surveillance Capitalism." *Orangespace*, February 15, 2019. https://blaynehaggart.com/2019/02/15/evaluating-scholarship-or-why-i-wont-be-teaching-shoshana-zuboffs-the-age-of-surveillance-capitalism/.

Haggerty, K.D. and Ericson, R.V. "The surveillant assemblage." *The British Journal of Sociology*, 51 (2000): 605-622. https://doi.org/10.1080/00071310020015280.

Hawkins, Derek. "The Cybersecurity 202: Why a privacy law like GDPR would be a tough sell in the U.S." *The Washington Post*, May 25, 2018. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/25/the-cybersecurity-202-why-a-privacy-law-like-gdpr-would-be-a-tough-sell-in-the-u-s/5b07038b1b326b492dd07e83/.

Holloway, Donell. "Surveillance capitalism and children's data: the Internet of toys and things for children." *Media International Australia* 170, no. 1 (February 2019): 27-36. https://doi.org/10.1177/1329878X19828205.

"How much is 1 byte, kilobyte, megabyte, gigabyte, etc.?" *Computer Hope*, August 31, 2020. https://www.computerhope.com/issues/chspace.htm.

Hudson, Rob. "Fordism." In *International encyclopedia of human geography. 7. Me - N*, 226-231. 2009.

Jessop, Bob. "Fordism." *Encyclopedia Britannica*, April 1, 2013. https://www.britannica.com/topic/Fordism.

Knake, Robert K. "Why the SolarWinds Hack is a Wake-Up Call." *Council on Foreign Relations*, March 9, 2021. https://www.cfr.org/article/why-solarwinds-hack-wake-call.

Kshetri, Nir. "Big data's impact on privacy, security and consumer welfare." *Telecommunications Policy* 38, no. 11 (December 2014): 1134-1145. https://doi.org/10.1016/j.telpol.2014.10.002.

Laney, Doug. "3D Data Management: Controlling Data Volume, Velocity, and Variety." *Garner*, 2001. http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.

*Law in United States*. Data Protection Laws of the World, 2021. https://www.dlapiperdataprotection.com/index.html?t=law&c=US&c2=.

Lee, Hakyung Kate. "South Korea's Contact Tracing Sheds Light on Extensive Efforts to Slow Spread of COVID-19." ABC News. December 9, 2020. https://abcnews.go.com/International/south-koreas-contact-tracers-struggle-slow-spread-covid/story?id=74621480.

Lehtiniemi, Tuukka. "Personal Data Spaces: An Intervention in Surveillance Capitalism?" *Surveillance & Society* 15, no. 5 (2017): 626-639. https://doi.org/10.24908/ss.v15i5.6424.

Lyon, David. “Surveillance Capitalism, Surveillance Culture and Data Politics.” In *Data Politics: Worlds, Subjects, Rights*, edited by Didier Bigo, Engin Isin, and Evelyn Ruppert, 74-88. New York: Routledge, 2019. https://scholar.googleusercontent.com/scholar?q=cache:g5SP02_tuGwJ:scholar.google.com/+social+media+and+surveillance+capitalism&hl=en&as_sdt=0,10&as_vis=1.

Ma, Alexandra, and Ben Gilbert. “Cambridge Analytica: a Guide to the Trump Linked Data Firm That Harvested 50 Million Facebook Profiles.” *Business Insider*, March 17, 2018. https://www.businessinsider.com/cambridge-analytica-trump-firm-facebook-data-50-million-users-2018-3.

Malmgren, Evan. “Resisting ‘Big Other’: What Will It Take to Defeat Surveillance Capitalism?” *New Labor Forum* 28, no. 3 (2019): 42-50. https://doi.org/10.1177/1095796019864097.

Marshall, William F. “Can Contact Tracing Stop Coronavirus?” *Mayo Clinic*, December 15, 2020. https://mayoclinic.org/diseases-conditions/coronavirus/expert-answers/covid-19-contact-tracing/faq-20488330.

McKenna, Josephine. “Big data: big promise.” *European Heart Journal* 38, no. 7 (February 14, 2017): 470-471. https://doi-org.ezproxy.bu.edu/10.1093/eurheartj/ehx021.

*Merriam-Webster.com Dictionary*, s.v. “capitalism,” accessed April 22, 2021, https://www.merriam-webster.com/dictionary/capitalism.

Meza, Summer. “Zuckerberg spent an absurd amount of time explaining how the internet works in his Senate testimony.” *The Week*, April 10, 2018. https://theweek.com/speedreads/766564/zuckerberg-spent-absurd-amount-time-explaining-how-internet-works-senate-testimony.

Nemeth, Mitchell. “Will Privacy Continue to Take a Backseat to Surveillance Capitalism.” *Medium*, January 25, 2020. https://towardsdatascience.com/will-privacy-continue-to-take-a-backseat-to-surveillance-capitalism-9cd6fc6b597c.

Niebel, Thomas, Fabienne Rasel, and Steffen Viete. “BIG Data - BIG Gains? Understanding the Link between Big Data Analytics and Innovation.” *Economics of Innovation and New Technology* 28, no. 3 (2019): 296-316. https://doi.org/10.1080/10438599.2018.1493075.

Park, Sangchul, Gina J. Choi, and Haksoo Ko. "Information Technology–Based Tracing Strategy in Response to COVID-19 in South Korea—Privacy Controversies." *Jama Network*, April 2020. https://jamanetwork.com/journals/jama/fullarticle/2765252.

Patterson, Dan. "Dark Web: A cheat sheet for business professionals." *TechRepublic*, October 26, 2018. https://www.office1.com/blog/horror-stories-from-the-dark-web.

Prescott, Natalie A. "The Anatomy of Biometric Laws: What U.S. Companies Need To Know in 2020." *The National Law Review*, November 7, 2020. https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020.

"Privacy policy." *Omegle*, June 3, 2014. https://www.omegle.com/static/privacy.html.

Rabang, Imelda. "Living in the Age of Surveillance is a Modern-Day Threat." *Bold Business*, August 29, 2019. https://www.boldbusiness.com/digital/surveillance-capitalism/.

Sauer, Lauren M. "What Is Coronavirus?" *Johns Hopkins Medicine*, accessed April 22, 2021. https://www.hopkinsmedicine.org/health/conditions-and-diseases/coronavirus.

Schiappa, Daniel. "The Big Business of Cybercrime: The Dark Web." *Forbes*, September 12, 2019. https://www.forbes.com/sites/forbestechcouncil/2019/09/12/the-big-business-of-cybercrime-the-dark-web/?sh=61cdd9a15142.

Scott, James. "Equifax: The Hazards of Dragnet Surveillance Capitalism." *Institute for Critical Infrastructure Technology*, (October 2017): 1-17. https://icitech.org/wp-content/uploads/2017/10/ICIT-Analysis-Equifax-The-Hazards-of-Dragnet-Surveillance-Capitalism.pdf.

Shaw, Johnathon. "The Watchers." *Harvard Magazine,* December 18, 2016. https://harvardmagazine.com/2017/01/the-watchers.

Silverman, Jacob. "How Tech Companies Manipulate Our Personal Data." Review of *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, by Shoshana Zuboff. *The New York Times*, January 18, 2019. https://www.nytimes.com/2019/01/18/books/review/shoshana-zuboff-age-of-surveillance-capitalism.html.

Singer, Natasha. "The Week in Tech: How Google and Facebook Spawned Surveillance Capitalism." *The New York Times*, January 18, 2019.

https://www.nytimes.com/2019/01/18/technology/google-facebook-surveillance-capitalism.html.

Sonn, Jung Won. "Coronavirus: South Korea's success in controlling disease is due to its acceptance of surveillance." *The Conversation*, March 19, 2020. https://theconversation.com/coronavirus-south-koreas-success-in-controlling-disease-is-due-to-its-acceptance-of-surveillance-134068.

"Sources of big data: Where does it come from?" *CloudMoyo*, accessed April 18, 2021. https://www.cloudmoyo.com/blog/data-architecture/what-is-big-data-and-where-it-comes-from/.

Thompson, Derek. "Why Surveillance Is the Climate Change of the Internet." *The Atlantic*, May 9, 2019. https://www.theatlantic.com/ideas/archive/2019/05/crazygenius-season-three-privacy-internet/589078/.

Thompson, G. F. "Fordism, Post-Fordism, and the Flexible System of Production." Accessed April 22, 2021. https://www.cddc.vt.edu/digitalfordism/fordism_materials/thompson.htm.

Tibken, Shara. "Questions to Mark Zuckerberg show many senators don't get Facebook." *CNET*, April 11, 2018. https://theweek.com/speedreads/766564/zuckerberg-spent-absurd-amount-time-explaining-how-internet-works-senate-testimony.

*United States V. New York Telephone Co., 434 U.S. 159 (1977)*. Accessed April 20, 2021. https://supreme.justia.com/cases/federal/us/434/159/.

U.S. Congress. Senate. Committee on Commerce, Science, and Transportation. *Consumer Online Notification for Stopping Edge-provider Network Transgressions or the CONSENT Act: Summary (to Accompany S.2639)*. 115th Cong., 2d sess., 2018. S. Doc. https://www.congress.gov/115/bills/s2639/BILLS-115s2639is.pdf.

Wake, Ciara. "3 Ways That Social Media Knows You Better Than Your Friends and Family Do." Loyola Emerging Media 360. Last modified 2017. Accessed April 15, 2021. https://www.loyola.edu/academics/emerging-media/blog/2017/3-ways-that-social-media-knows-you-better-than-your-friends-and-family-do#:~:text=By%20tracking%20users%20Facebook%2C%20Instagram,of%20what%20your%20inerest%20are.&text=By%20using%20the%20location%20services,you%20are%20at%20all%20times.

Whelan, Glen. “Trust in Surveillance: A Reply to Etzioni.” *Journal of Ethics* 156, no. 4 (April 2019): 15-19. https://doi.org/10.1007/s10551-018-3779-4.

“What We Do,” *Federal Trade Commission*, accessed April 20, 2021. https://www.ftc.gov/about-ftc/what-we-do.

“Why Apple Is Right to Challenge an Order to Help the F.B.I.” *The New York Times*, February 19, 2016. https://www.nytimes.com/2016/02/19/opinion/why-apple-is-right-to-challenge-an-order-to-help-the-fbi.html.

Wolfard, Ben. “What is GDPR, the EU’s new data protection law?” *GDPR EU*. https://gdpr.eu/what-is-gdpr/. Accessed April 23, 2021

Yeung, Karen. “‘Hypernudge’: Big Data as a mode of regulation by design.” *Information, Communication & Society* 20, no. 1 (2017): 118-136. https://doi.org/10.1080/1369118X.2016.1186713.

Zastrow, Mark. “South Korea is Reporting Intimate Details of COVID-19 Cases: Has It Helped?” *Nature*, March 18, 2020. https://www.nature.com/articles/d41586-020-00740-y.

Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.

Zuboff, Shoshana. “Big other: surveillance capitalism and the prospects of an information civilization.” *Journal of Information Technology* 30, (April 4, 2015): 75-89. https://ssrn.com/abstract=2594754.

Zuboff, Shoshana. “Surveillance Capitalism Has Gone Rogue. We Must Curb Its Excesses.” *The Washington Post*, January 24, 2019. https://www.washingtonpost.com/opinions/surveillance-capitalism-has-gone-rogue-we-must-curb-its-excesses/2019/01/24/be463f48-1ffa-11e9-9145-3f74070bbdb9_story.html.

Zuboff, Shoshana, Guillaume Chaslot, and Ramesh Srinivasan. “The Perilous Power of Social Media Platforms.” Interview by Jonathan Chang and Meghna Chakrabarti. *WBUR*, NPR, February 04, 2021. Audio, 46:54. https://www.wbur.org/onpoint/2021/02/04/the-perilous-power-of-social-media-platforms.