50 Attorneys General Investigate Google: Surveillance Capitalism and Legal Privacy Frameworks

Brian Keogh

I. 50 STATE ATTORNEYS GENERAL INVESTIGATE GOOGLE

On September 9, 2019, fifty Attorneys General, less California and Alabama, launched an investigation against Google for antitrust violations related to Google's advertising business "and use of consumer data."[1]

Although personal data often appears in the news (especially in relation to security breaches)[2] the fact is most of us never ask what really happens to our data. The convenience and simplicity of using Google are the tip of the iceberg when it comes to the average users'[3] interactions with Google. All the data Google collects underneath the surface is easy for the user to forget about. Users only realize what they have traded when something goes wrong. Google's ambition is to amass and analyze this data to achieve something approaching omniscience and relies upon users' inability to control their data. Google's ambitious project may be a pyramid that individual users neither need nor want, or more generally, a project that humanity neither needs nor wants. While this Note will not advocate for Google to be considered a utility or for its breakup, its ubiquitous status in our culture and actual utility put users at a significant disadvantage when interacting with the company. An unsustainable imbalance exists.

The answer lies in a privacy law that balances the interests of companies like Google with the interests of their users. The current state of affairs demands that the scales be balanced back in favor of users to correct a growing power imbalance. The United States should, at the very least, adopt regulation equivalent to the European Union's General Data Protection Regulation. As we will see, it should perhaps consider adopting even greater protection.[4]

As things stand, compared to the EU data privacy regime, the General Data Protection Regulation[5], the United States cannot protect its consumers

---

[1] Lauren Feiner, *Google Faces a New Antitrust Probe by 50 Attorneys General*, CNBC (Sept. 9, 2019, 2:05 PM), https://www.cnbc.com/2019/09/09/texas-attorney-general-leads-google-antitrust-probe.html.

[2] These are too numerous to detail here; however, many businesses have come under fire for failing to secure users' information, especially credit card information and social security numbers—perhaps most famously, Facebook and Cambridge Analytica (although these specific breaches did not include credit card information or SSNs).

[3] This Note will refer to the people using Google search, Gmail, Google Maps, or other services as users. Google's customers are the people and businesses who pay for (mostly) its advertising services- advertisers. *Infra* III; Shoshana Zuboff, *Surveillance Capitalism and the Challenge of Collective Action*, 28 NEW LAB. F. 10, 21 (2019)("surveillance capitalists no longer rely on people as consumers. Instead, the axis of supply and demand orients the surveillance capitalist firm to businesses intent on anticipating the behavior of populations, groups, and individuals. The result is that populations are conceptualized as undifferentiated 'users,' who are merely the sources of raw material for a digital-age production process aimed at a new business customer.").

[4] *Infra* IV.C.

[5] General Data Protection Regulation (EU) 2016/679, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN [hereinafter GDPR].

and citizens because it lacks a coherent authority and policy to do so.[6] Antitrust law may alleviate some problems but may not be enough given the enormous economic benefits AI and data analysis can provide.[7]

It is the purpose of this Note to point out that the law should take into consideration whether a firm's business model relies upon "human experience as free raw material for hidden commercial practices of extraction, prediction, and sales" or what will be referred to as "surveillance capitalism" throughout this Note.[8] At some point, in a market as profitable as user data, the United States ought to "provide that everyone has the right to the protection of personal data concerning him or her."[9] The European Union (EU) legislation demonstrates one way to balance interests between surveillance capitalists and users and it falls to the United States to adopt and adapt in a similar way for the benefit of its citizens.

II. ORIGINS OF DATA PRIVACY AND THE RISE OF GOOGLE

Google entered into conflict with privacy at its inception. Google's search engine wants to be able to find everything and no one can deny its awesome utility, even if society can occasionally make fun of its less sensical or relevant results.[10] Given its overwhelming functionality and our growing inability to answer a question without it, if the cost is only our personal data and our privacy, why should we care?

A. Why care about privacy?

What to do with consumers' data is a question that has been around for some time. "[T]he necessity to create particular legal frameworks emerged from the growing importance of electronic data processing in the 1960s and 1970s."[11] It is data collection through surveillance capitalism that interferes with privacy, which is "[a]n intermediate value for other human rights and an essential means for identity-building, which fosters liberty, autonomy and self-determination."[12] These are all factors a democratic society needs or the *sine qua non* of democracies.[13]

---

[6] ERIN J. ILLMAN & S. DAVID SMITH, SCOPE OF U.S. PRIVACY LAW TODAY, 2018 TXCLE-ACCL 1-II, 2018 WL 6687719.

[7] *Technology Firms Vie for Billions in Data-Analytics Contracts*, ECONOMIST (Sept. 5, 2019), https://www.economist.com/business/2019/09/05/technology-firms-vie-for-billions-in-data-analytics-contracts.

[8] SHOSHANA ZUBOFF, SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019).

[9] GDPR, *supra* note 5.

[10] *See Wired Autocomplete Interviews*, WIRED, https://www.wired.com/video/series/google-autocomplete-inverviews (last visited May 5, 2021) (interviews in which celebrities comment on Google suggested search queries about themselves).

[11] STEFAN STRAUSS, PRIVACY AND IDENTITY IN A NETWORKED SOCIETY, 47 (2019).

[12] *Id.*

[13] *Id.* at 54.

"[P]rivacy provides an environment for the free flow of personal information, where this information is (ideally) not disclosed or accessible to other entities unless intended to be by the individual concerned."[14] Privacy allows human beings to regulate between private and public spheres; it is "a vital societal function" and "it has an inherent boundary control function."[15] "[P]rivacy protection basically regulates informational relations and boundaries between individuals and other entities."[16]

Our connections have become increasingly digital, and as a consequence, our social lives play out across networked publics.[17] However, through their interactions with Google, Facebook, Instagram, Snapchat, and Twitter, the youngest generations are accustomed and socialized to expect and accept less privacy.[18] The United States lacks privacy protections which would likely allow programs like China's social scoring systems.[19] Ultimately, human dignity is at stake[20] along with democracy because privacy is essential for democracy at the individual and societal level.[21]

B. OECD Guidelines

Despite its importance, privacy is an issue that, while the world saw coming, it underprepared for.[22] Germany, France, Sweden, and the United States all created privacy laws in the 1970s.[23] In 1980, the OECD established guidelines to privacy including eight principles for the processing of data.[24] Both the EU and United States endorsed the Organization for Economic Co-Operation and Development's (OECD) recommendations to "protect personal data and the fundamental right to human privacy."[25]

The United States and EU both agreed in principle under the "Individual Participation Principle" that individuals should be able 1) to confirm whether

---

[14] *Id.* at 55.

[15] *Id.* at 263.

[16] *STRAUSS, supra* note 11, at 264.

[17] ZUBOFF, *supra* note 8, at 455.

[18] Tiffany Kim, *Younger Generations are Infected by Continuous Socialization to Accept Diminished Privacy: A Global Analysis of How the United States' Constitutional Doctrine is a Main Contributor to Eroded Privacy*, 26 IND. J. GLOBAL LEGAL STUD. 335 (2019).

[19] *Id.* at 352.

[20] ZUBOFF, *supra* note 8, at 522 (describing how the 'bare facts' of surveillance capitalism demean human dignity and threaten a human future).

[21] STRAUSS, *supra* note 11, at 264.

[22] STRAUSS, *supra* note 11, at 47.

[23] *Id.*

[24] *How Did We Get Here?*, EUGDPR.ORG, https://eugdpr.org/the-process/how-did-we-get-here/ (last visited May 5, 2021) (The OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data proposed eight principles for the processing of data); *see also* STRAUSS, *supra* note 11, at 47.

[25] *Id.*; *see also* STRAUSS, *supra* note 11, at 47.

someone has data about them; 2) to request that data about them be communicated; 3) to be told why, in the event the entity with their data denied their request and to challenge the denial; and 4) "to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended."[26] In between attempts to make guidelines and rules, the internet and Google arrived in our homes and our phones.

C. Google

In 1998, Google came into existence at Stanford.[27] It quickly became known for its search function. In common parlance, 'Google' replaced 'search' as a verb and was duly added to the Oxford English Dictionary.[28] In 2017, two billion people used Android devices, and one billion monthly active users were on Gmail, Android, Chrome, Maps, Search, YouTube, and the Google Play Store.[29] But going back to the beginning, it was not the money Google made directly from users making searches that transformed Google into one of the most valued companies in the world, but its advertising business.

Google's actual business is advertising. While it provides many useful functions to its users, such as search, these functions allow Google to collect its users' data and monetize the information. [30] Google chose to pursue an advertising model instead of a fee model.[31] There is no question that Google provides excellent tools but while "[t]he tools on offer by Google and other surveillance capitalist firms respond to the needs of beleaguered second modernity individuals—like the apple in the garden, once tasted they are impossible to live without."[32] Google's investments in user services were made so that users would continue to supply Google with what its customers – advertisers – wanted, the online behavior surplus of the users.[33] Hal Vairan, Google's chief economist in 2009, described Google as "giving away products" because "use" and "eyeballs" lead to more sales for Google. [34] Google's advertising software found a niche that made it essential to anyone placing an ad online, those not using it are "out in the cold, relegated to a tiny, irrelevant

---

[26] ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA 15, (1980), https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

[27] ERIC SCHMIDT & JONATHAN ROSENBERG, HOW GOOGLE WORKS 4 (2014) (stating that Sergey Brin and Larry Page founded Google in 1998 with the goal of creating world's best search engine).

[28] *Id.* at 3.

[29] ZUBOFF, *supra* note 8, at 400–01.

[30] *Id.* at 88.

[31] Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75, 79 [hereinafter *Big Other*](stating that Google's success in this area is a driver of "big data analytics").

[32] *Id.* at 83.

[33] ZUBOFF, *supra* note 8, at 88.

[34] *Big Other*, *supra* note 31, at 79.

subculture."[35] After using clicks to measure success, Google began to develop new ways to analyze and extract data.[36] Google's discovery of ways to take data and sell it through ranked advertising exposed the world to surveillance capitalism.[37] Google takes that data from its users, and its users are "the *objects* from which raw materials are extracted and expropriated for Google's prediction factories."[38] Varian described the collection of user data as extraction—a one way process.[39] Google describes itself, though, as setting out to solve the entire planet's big problems.

Google luminaries Eric Schmidt and Jonathan Rosenberg see "most big problems as information problems."[40] They both hold to Google's belief that "with enough data and the ability to crunch it, virtually any challenge facing humanity today can be solved."[41] What they describe is Google's hunger for data and its desire to collect everything from weather data to a person's vital signs—tracked by a Google device, of course.[42] To this end, Google announced its acquisition of Fitbit for $2.1 billion dollars in November 2019.[43] This is not the only activity Google is engaged in in the healthcare industry. Google is working with Ascension, which operates 2,600 healthcare facilities, including hospitals and doctor's offices, to process the data of tens of millions of patients.[44] Although likely permissible under federal law, the Health Insurance Portability and Accountability Act of 1996, this collection was all done secretly without doctor or patient knowledge.[45] This is allowable provided the data is only being used to help Ascension carry out its health care function.[46] In reality, the acquisition is a field test or experiment for Google's

[35] JARON LANIER, YOU ARE NOT A GADGET 15 (2011).

[36] ZUBOFF, *supra* note 8, at 83.

[37] *Id.* at 85.

[38] *Id.* at 94.

[39] *Id.* at 83; *Big Other*, *supra* note 31, at 79.

[40] SCHMIDT & ROSENBERG, *supra* note 27, at 256.

[41] *Id.*

[42] *Id.*

[43] Rachel Siegel & Tony Romm, *Google Will Acquire Fitbit in a Direct Challenge to Apple*, WASH. POST (Nov. 1, 2019, 9:34 AM), https://www.washingtonpost.com/technology/2019/11/01/google-will-acquire-fitbit-billion-deal-direct-challenge-apple/ ("Fitbit gives consumers immediate access to ever-more-specific slices of fitness data — from their daily step count to their heart rate to how well they sleep. Yet the data has also become a treasure trove for employers and insurance companies, complicating the relationships between workers and their bosses.").

[44] Rob Copeland, *Google's 'Project Nightingale' Gathers Personal Health Data on Millions of Americans*, WALL ST. J. (Nov. 11, 2019, 4:27 PM), https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790.

[45] *Id.*

[46] *Id.*

AI and machine learning programs.[47] Google Fitbit believes the data it collects "will not be used for Google ads."[48] Because of the pending investigations and steadily increasing scrutiny of Google, the deal includes a $250 million pay-out to Fitbit if regulators veto it.[49]

Why risk $250 million? Google believes that the benefits of the free flow of information trump any individual right to privacy.[50] If that information solves all of humanity's problems it may even seem like a small price. Google previously determined to not disclose to users an issue that exposed birth dates in order to not trigger regulatory scrutiny.[51] Informing users was unnecessary because Google went beyond legal requirements in making its decision.[52]

While Google's view of humanity's ability to solve world problems is optimistic, it is a blind utilitarian belief that discounts and fails to address what rights other parties have. It suggests we should shut up and be grateful 'smart creatives' will take our information and eventually solve society's problems after lining their pockets.[53] On the other hand, Larry Page put users' privacy concerns in this context: "We're not really thinking about the tremendous good that can come from people sharing information with the right people in the right ways." [54] Technological progress is an important consideration and self-regulation for newer areas makes sense, but after 20 years Google should come to terms with the need for the regulation of data privacy and assist or let a baseline be established.[55]

Google's business began facing the first serious legal pushback to its hunger for data in Europe and when the EU passed the GDPR and in the EU, users were not only protected by the law but granted rights.

D. European GDPR

In Europe, the General Data Protection Regulation (GDPR) aims to "protect and empower all EU citizens data privacy."[56] The GDPR went into

---

[47] *See generally* David M. Parker et al., *Privacy and Informed Consent for Research in the Age of Big Data*, 123 PA. STATE L. REV. 703, 705 (2019)(addressing a middle ground for Big Data and how it is used in research by balancing social interests and autonomy).

[48] Siegel & Romm, *supra* note 43.

[49] *Id.*

[50] Schmidt & Rosenberg, *supra* note 27, at 256.

[51] Copeland, *supra* note 44.

[52] *Id.*

[53] *Id.*

[54] *Id.*

[55] ROXANA RADU, NEGOTIATING INTERNET GOVERNANCE 157 (2019).

[56] GDPR.ORG, https://gdpr.eu/ (last visited Mar. 14, 2021).

effect May 2018.[57] Prior to its enactment, European courts put the brakes on Google's activities.

In Spain, the Court of Justice of the European Union established that users could request the removal of their information from search engines.[58] Another unfavorable outcome to Google was the highest EU court striking down the Safe Harbor agreement because the United States had lower privacy standards than the EU.[59] The Safe Harbor agreement allowed U.S. companies to certify their own protections (policies and procedures for handling data) satisfied EU law to allow them to transfer EU users' data to the United States.[60] The EU Court of Justice determined that the right to privacy trumped the free flow of information.[61] Since then, the "Privacy Shield" replaced the Safe Harbor agreement.[62] This new agreement is currently under scrutiny for its safeguards to government access of user data.[63]

The GDPR restrictions "show that the European Union placed more of a premium on universally protecting what it considered to be a fundamental right to exclusive ownership of personal information absent legal necessity or explicit consent otherwise by the subject."[64]

In part, the GDPR establishes the following:

> (1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.[65]

Right away it becomes clear that "providing EU residents," or "data subjects," with more control over their personal data through a suite of individual data rights; and requiring accountability mechanisms that govern the lawful

---

[57] *How did We Get Here?*, EUGDPR.ORG, https://eugdpr.org/the-process/how-did-we-get-here/ (last visited Mar. 14, 2021).

[58] RADU, *supra* note 55, at 142.

[59] *Id.* (stating that the decision upended "data transfers to non-EU countries based on a guarantee of 'adequate protection'").

[60] Dylan Cors, *National Security Data Access and Global Legitimacy*, 67 DOJ J. FED. L. & PRAC. 257, 260 (2019).

[61] ZUBOFF, *supra* note 8, at 59.

[62] Cors, *supra* note 60, at 260.

[63] *Id.* (arguing that in this area of national security, U.S. law can withstand scrutiny regarding how the U.S. government handles foreign customers data).

[64] John Schinasi, *Practicing Privacy Online: Examining Data Protection Regulations Through Google's Global Expansion*, 52 COLUM. J. TRANSNAT'L L. 569, 589 (2014).

[65] GDPR, *supra* note 5, at 1.

processing of personal data is regarded differently in Europe and is a "fundamental right."[66]

> (2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.[67]

The GDPR clearly lays out the principle behind its citizens' rights. EU citizens have a right to the protection of their personal data and the processing of that data.[68] Data processing should be designed to serve the users.[69] It is not meant to be an absolute right[70] but given the interaction of privacy with the public and private spheres of life the protection is one that must be weighed carefully.[71] Its most innovative aspects include "the focus on the explicit consent of the user, the right to rectification and erasure of information, as well as the right to explanation."[72]

The GDPR gave users teeth. As an enforcement mechanism, "the GDPR permits fines up to four percent of a company's worldwide revenue or twenty million Euros, whichever is greater," to be imposed on companies found to be in violation of the law.[73] Article 80 of the GDPR allows users to designate non-profit organizations or non-governmental organizations to enforce the law.[74]

Subsequently, on January 22nd, 2019, France fined Google $57 million for violating the GDPR.[75] It is the first such decision under the GDPR.[76] In the

---

[66] Joseph Jerome, *California Privacy Law Shows Data Protection Is on the March*, 33 ANTITRUST 96 (2018).

[67] GDPR, *supra* note 5, at 1.

[68] *Id.*

[69] *Id.* at 2.

[70] *Id.* ("[The right] must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.").

[71] STRAUSS, *supra* note 11, at 264.

[72] RADU, *supra* note 55, at 167.

[73] Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 776 (2019).

[74] *Id.* at 776–77.

[75] Tony Romm, *France Fines Google Nearly $57 Million for First Major Violation of New European Privacy Regime,* WASH. POST (Jan. 21, 2019), https://www.washingtonpost.com/world/europe/france-fines-google-nearly-57-million-for-first-major-violation-of-new-european-privacy-regime/2019/01/21/89e7ee08-1d8f-11e9-a759-2b8541bbbe20_story.html.

[76] *Id.*

United States, users lack such protections, despite U.S. support for the ideas the OECD put forth in 1980.[77]

There is instead an inconsistent patchwork of laws across all 50 states and an emphasis on self-regulation.[78] The European Commission views self-regulation as a failure.[79] As a result of the regulation in Europe, Google is held to account in European Courts.[80] Under the current patchwork in the United States, it is difficult for users to find recourse in the courts and the companies falling under various regulations want a comprehensive omnibus to follow.

E. United States Regulation

In the United States there is not a right to the processing of data or any kind of comprehensive law regulating the collection of data as it relates to privacy. "In the United States, there is no single, comprehensive national law regulating the collection and use of personal data."[81]

Instead, multiple agencies enforce privacy laws, including the Federal Trade Commission, Department of Health and Human Services, Securities and Exchange Commission, Federal Communications Commission, Consumer Financial Protection Bureau, State Attorneys General, and the New York Department of Financial Services.[82] These agencies enforce a wide range of laws:

> • The Federal Trade Commission Act(FTC Act)--prohibits unfair or deceptive practices and is frequently applied to privacy and data security policies and business practices.
>
> • The Financial Services Modernization Act(Gramm-Leach-Bliley Act (GLBA))--applies broadly to financial institutions (as well as businesses that provide financial services and products) and regulates the collection, use, and disclosure of financial information.
>
> • The Health Insurance Portability and Accountability Act(HIPAA)--applies broadly to healthcare providers, data processors, and other entities that handle medical data.
>
> • The Fair Credit Reporting Act(and the Fair and Accurate Credit Transactions Act)--applies to consumer reporting agencies, companies that use consumer reports, and companies that provide consumer-reporting information.

---

[77] How Did We Get Here?, *supra* note 24.

[78] ILLMAN & SMITH, *supra* note 6.

[79] Schinasi, *supra* note 64, at 590.

[80] Romm, *supra* note 75.

[81] ILLMAN & SMITH, *supra* note 6.

[82] *Id.*

- Electronic Communications Privacy Act--regulates the interception of electronic communications.[83]

As the five examples above demonstrate, the United States regulates specific areas of personal data and privacy instead of granting users fundamental rights when it comes to how their data is handled.[84] This sort of framework leads to problems when users bring litigation against companies like Google.

i. Case Law

As a result of this status quo, U.S. courts have not recognized an existing fundamental right to privacy users have in their data.[85] Accordingly, users may be unable to show that they have a "loss."[86] For example, in a 2015 case against Google, the court determined a reasonable factfinder could find that Google acted deceitfully; but on other claims that users brought against Google, the court determined that plaintiffs were not entitled to relief because the loss or taking of their data did not cause them damage under the Computer Fraud and Abuse Act (CFAA).[87] The court reasoned that the users' argument lacked "traction" because users could not show that they intended to participate or had participated in the market of user data.[88] Perhaps if the users alleged they wished to monetize this information the court would have come to a different conclusion.[89] This is an odd result given the economic market. Effectively, we trade our data for access to Google's services. Consequently, one of the biggest companies in the world exists and makes most of its money from its business selling precisely this data to advertisers. Many of these services are "free" precisely because the company uses user data to make a profit. But one company's gold is a user's trash, apparently.[90] Still, users saw part of the district court's ruling vacated because of Google's practice of overriding user cookie blockers.[91]

---

[83] *Id.*

[84] *Contra* GDPR, *supra* note 5.

[85] In re Google Inc. Cookie Placement Consumer Privacy Litig., 806 F.3d 125, 153 (3d Cir. 2015).

[86] *Id.* at 153 (noting that the lower court's dismissal of certain allegations was upheld because users could not show loss or sale as required by California statutes).

[87] *Id.* at 149.

[88] *Id.*

[89] *Id.*

[90] *Contra id.* (The court notes that users had no revenue from their data and could therefore show no loss or damages). *See generally* Gregory Barber, *Oasis Labs' Dawn Song on a Safer Way to Protect Your Data*, WIRED (Nov. 8, 2019), https://www.wired.com/story/dawn-song-oasis-labs-data-privacy-wired25/ (describing a startup that seeks to secure data after it is shared and to preserve its monetary value, a technology as a means of creating data protection).

[91] In re Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d at 151.

Consumer and states' concerns about Google's activities are being pursued by states' attorneys general in antitrust and consumer privacy investigations.[92] Overall, the United States takes what can be called a "harm-based" approach to the privacy and security of its users.[93] The United States only polices certain types of information or areas where the information is considered sensitive and where limits on collection, use, or sharing on data are imposed (e.g., financial and health).[94] This is in stark contrast to the GDPR which "attempts to cover everyone and everything and is less focused on whether or not individuals are ever even harmed by industry data collection and use."[95]

Cases that raise Fourth Amendment issues in the United States also fail to adequately protect the privacy or data of users.[96] "Applying technologies and situations in the information age against the current doctrinal backdrop contributes to the deterioration of information privacy because the application lacks adequate protections for individual privacy."[97] None of the current tests, including "[t]he reasonable expectation of privacy test, the content-or-no-content distinction, and the Third-party Doctrine" satisfy the concerns of the present day.[98] The gap in privacy exists not just between users and Google but between users and government.

Senator Amy Klobuchar introduced national legislation in the Senate entitled the "Social Media Privacy Protection and Consumer Rights Act of 2019." [99] This legislation seeks to "[improve] transparency, strengthen[] consumers' recourse options when a breach of data occurs, and ensur[e] companies are compliant with privacy policies that protect consumers."[100] The legislation would:

- Give consumers the right to opt-out and keep their information private by disabling data tracking and collection,
- Provide users greater access to and control over their data,

---

[92] Brent Kendal, *Attorneys General Launch Probe of Google*, WALL ST. J. (Sept. 9, 2019, 5:08 PM), https://www.wsj.com/articles/attorneys-general-launch-probe-of-google-11568055853.

[93] Jerome, *supra* note 66, at 96.

[94] *Id.*

[95] *Id.*

[96] *But see* Carpenter v. United States, 138 S. Ct. 2206 (2018)(describing limits on the government).

[97] Kim, *supra* note 18, at 351–52 (reasoning that the Court "is operating on a circular analysis of societal expectations").

[98] *Id.*

[99] Social Media Privacy Protection and Consumer Rights Act of 2019, S. 189, 116th Cong. (2019).

[100] *Klobuchar, Kennedy Introduce Bipartisan Legislation to Protect Privacy of Consumers' Online Data*, SEN. AMY KLOBUCHAR, https://www.klobuchar.senate.gov/public/index.cfm/2019/1/klobuchar-kennedy-introduce-bipartisan-legislation-to-protect-privacy-of-consumers-online-data (last visited Jan. 16, 2021).

- Require terms of service agreements to be in plain language,
- Ensure users have the ability to see what information about them has already been collected and shared,
- Mandate that users be notified of a breach of their information within 72 hours,
- Offer remedies for users when a breach occurs,
- Require that online platforms have a privacy program in place.[101]

This proposed legislation demonstrates that in some ways the United States may be approaching the GDPR. Americans like Klobuchar are coming to understand the realities of surveillance capitalism and that "[e]very day, companies profit off of the data they're collecting from Americans, yet leave consumers completely in the dark about how their personal information, online behavior, and private messages are being used. Consumers should have the right to control their personal data." [102] Even tech companies are acknowledging the need for national legislation. "We really, really, support an omnibus federal privacy law."[103] In response to voters, California is moving in that direction with its own law regulating privacy.

ii. State Law of California 2020

Ultimately, California's law (CCPA) may pave the way for the federal government to establish a floor for a right to privacy.

It provides for a "right to be forgotten," what companies need to tell users, etc.[104] Functionally, it rhymes with the GDPR.[105] However, "whereas the GDPR embraces concepts like data minimization and purpose specification, there are several provisions in the CCPA that actually promote expansive uses of information by businesses."[106] It does not establish the same protections as the GDPR, such as requiring "the appointment of corporate data-protection officers and assessments of the projects data-protection risks."[107]

Whatever its shortcomings, it may provide a signpost for the future of regulation in the United States and a way to address surveillance capitalism.

---

[101] *Id.*

[102] *Id.*

[103] *Companies Should Take California's New Data-Privacy Law Seriously*, ECONOMIST (Dec. 18, 2019), https://www.economist.com/business/2019/12/18/companies-should-take-californias-new-data-privacy-law-seriously (quoting a data-privacy official of a large American technology company).

[104] CAL. CIV. CODE § 1798.115 (West 2020); Cal. Assemb. B. 375, 2018 (Cal. 2018), https://leginfo-legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

[105] *Companies Should Take California's New Data-Privacy Law Seriously*, *supra* note 103.

[106] Jerome, *supra* note 66, at 96, 98.

[107] *How to Think About Data in 2019*, ECONOMIST (Dec. 22, 2018).

III. SURVEILLANCE CAPITALISM AND PRIVACY LAW

Surveillance capitalism describes the way Google takes data from its users, and then uses that data to create a prediction of user behavior, and that product makes Google its profit.[108] This business of data collection and behavior prediction is "the new oil."[109]

But what does surveillance capitalism tell us about the law? Essentially, that the law does not currently exist to prevent firms like Google from extracting data and profiting from "behavior" which represents a new commodity in the worldwide marketplace.

A. What is Surveillance Capitalism?[110]

Surveillance capitalism takes advantage of consumers ignorance and deprives them of choice.[111] Users, knowingly or not, provide Google with vast quantities of their data and personal information, allowing Google to not just deliver the most pertinent search result or advertisement but "more or less guess what you're thinking about."[112] The companies that collect and profit from the data users unwittingly give them have begun to change our notion of how businesses operate.[113] This new and massive type of business that relies on the tracking and selling of personal consumer data is "surveillance capitalism."[114]

Surveillance capitalism creates a fourth fictional commodity: behavior.[115] Other fictional commodities—land, labor, and money—are subjected to the law–property law, labor law, and banking law.[116] Until the GDPR, surveillance capitalism faced few meaningful regulations and only had to contend with guidelines and recommendations.[117] "Surveillance capitalists have skillfully exploited a lag in social evolution as the rapid development of their abilities to surveil for profit outrun public understanding and the eventual development of law and regulation that it produces."[118] Behavior is not just about prediction. "This is a new business frontier comprised of

---

[108] ZUBOFF, *supra* note 8, at 94.

[109] *Companies Should Take California's New Data-Privacy Law Seriously*, *supra* note 103.

[110] ZUBOFF, *supra* note 8, at 498 (detailing how surveillance capitalism differs from capitalism).

[111] *Big Other*, *supra* note 31, at 83.

[112] Brian Barth, *The Defector*, NEW YORKER 28 (Dec. 2, 2019)(quoting former Google chairman Eric Schmidt).

[113] *See generally* ZUBOFF, *supra* note 8. (In her book, Zuboff details how both Facebook and Google operate as surveillance capitalists. For the sake of brevity, Facebook is mostly absent from this Note, if not entirely).

[114] *Big Other*, *supra* note 31, at 83.

[115] ZUBOFF, *supra* note 8, at 514.

[116] *Id.*

[117] *See id.*

[118] *Big Other*, *supra* note 31, at 83.

knowledge about real-time behavior that creates opportunities to intervene in and modify behavior for profit."[119] That modification of behavior is a new kind of power, which Zuboff has termed "instrumentarianism": "the instrumentation and instrumentalization of human behavior for the purposes of modification, prediction, monetization, and control."[120]

The collection of user data is so large that everyone using Google's services inadvertently creates a digital self or "data voodoo doll."[121] This data becomes an extension of the user and this new raw resource, data, generated by the user, ought to be considered property.[122]

There is no reason for users to be content with this status quo and the manipulation of not just their data but their wills. This shaping of behavior is actuation.[123] 'Actuation' allows sensors to modify a person's behavior so that a person stops what they are doing or starts something they did not choose.[124] The devices we use, such as our smart phones, may allow us to be broadly conditioned.[125] The revenues companies like Google generate encourage "the continuous accumulation of more and more predictive forms of behavioral surplus."[126] To achieve this, Google needs to constantly experiment and improve its system to grasp causal knowledge.[127] We are unwitting guinea pigs in Google's experiment to modify our behavior for profit while it ignores any autonomy or self-determination we might have.[128]

What is the right source of law to regulate this new fictional commodity? Given the vast scope of data companies like Google intend to analyze and apply for what they consider to be our own good, comprehensive national protection is called for to regulate this area. State by state solutions are not enough, although they may be helpful or may serve as a model for federal regulation.

Rather it is through European courts and European legislation that privacy concerns are being addressed and in doing so are rejecting unregulated surveillance capitalism as a model.[129]

---

[119] *Id.* at 84. *But see* Barth, *supra* note 112 (describing the poor predictive power of fourteen data brokers "dire warnings about behavioral manipulation may not be entirely sound").

[120] Zuboff, *supra* note 3, at 20.

[121] Barth, *supra* note 112.

[122] *Id.* (taking a metaphor too far, critic of Big Tech, Roger McNamee, argues that it is "no more legitimate to trade the data in a data voodoo doll than it is to trade someone's kidney"). The salient point is that a user's interest in their data is not worthless, but in fact, very valuable.

[123] ZUBOFF, *supra* note 8, at 293 (quoting a senior software engineer "the real aim is ubiquitous intervention, action, and control").

[124] *Id.*

[125] *Id.* at 296.

[126] *Id.* at 297.

[127] *Id. at* 298.

[128] ZUBOFF, *supra* note 8, at 298.

[129] *Id.* at 59, 484, 514.

It is an interesting question if the results of the attorneys general investigation will reveal something about Google that is different from other firms engaging in market capitalism and distinguish this case to the courts. Surveillance capitalism is different from what economists usually think of capitalism insofar as, in part, "it insists on the privilege of unfettered freedom *and* knowledge."[130] "[Surveillance capitalism] is accomplished through a form of unilateral declaration that most closely resembles the social relations of a pre-modern absolutist authority . . . hyperscale becomes a profoundly anti-democratic threat."[131] Users give Google so much of their data and personal information that the invisible hand of the market is instead visible, meaning that Google knows what users will do before they do it, where they are, and what they are thinking about.[132]

The consequences of this surveillance are staggering. It grants those with the information the ability to observe previously unseen behavior and "write contracts on it."[133] Theoretically, according to Varian,

> If someone stops making monthly car payments, the lender can 'instruct the vehicular monitoring system not to allow the car to be started and to signal the location where it can be picked up.' Insurance companies, he suggests, can rely on similar monitoring systems to check if customers are driving safely and thus determine whether or not to maintain their insurance or pay claims. He also suggests that one can hire an agent in a remote location to perform tasks and use data from their smartphones – geolocation, time stamping, photos – to 'prove' that they actually performed according to the contract.[134]

We can say then that Google is being investigated because of "the asymmetry of power between surveillance capitalists and the societies in which they operate."[135] Surveillance capitalism interferes with privacy, which is "[a]n intermediate value for other human rights and an essential means for identity-building, which fosters liberty, autonomy and self-determination."[136] Google's platforms are everywhere and "[t]he result has been an involuntary merger of personal necessity and economic extraction, as the same channels that we rely on for daily logistics, social interaction, work, education, health care, access to products and services, and much more, now double as supply chain operations for surveillance capitalism's surplus flows."[137] Until the GDPR, surveillance

---

[130] *Id.* at 495.

[131] *Big Other*, *supra* note 31, at 83.

[132] ZUBOFF, *supra* note 8, at 498.

[133] *Big Other*, *supra* note 31, at 81.

[134] *Id.*

[135] ZUBOFF, *supra* note 8, at 499.

[136] STRAUSS, *supra* note 11.

[137] Zuboff, *supra* note 3, at 25.

capitalism faced few meaningful regulations and only had to contend with guidelines and recommendations.[138]

IV. HOW THE EU REGULATES GOOGLE'S SURVEILLANCE CAPITALISM AND HOW THE U.S. SHOULD

Through the GDPR, the EU has taken a step forward by regulating the fourth fictional commodity of behavior. It offers a comprehensive framework that avoids the pitfalls of the piecemeal approach the United States currently takes.

A. Current EU approach

Europe, particularly the EU, has more robust or finely detailed privacy rights. Google has already encountered the consequences of this. For instance, France enforced the EU's General Data Protection Regulation.[139]

The EU protects users' personal data from corporations but makes an exception for government action.[140] It creates a floor of protection which member states can expand upon.[141] It allows companies like Google to continue growing while giving users rights.[142] It may, however, present a burden to foreign small businesses competing in the digital economy.[143] The legal costs of complying and defending suits may be too burdensome for businesses of a certain size.[144] "[W]ith the advent of GDPR, [small businesses] decided to exit and only work in the United States. They did not have the resources to undergo GDPR compliance."[145] Privacy advocates argue that, in reality, the GDPR does not go far enough and that the GDPR requirement that users opt in to data processing by third parties results in consent to the status quo.[146]

B. U.S. v. EU.

The United States is now in a position where it will likely follow the lead of the EU given the fragmented state of the law in the United States.

While the United States once supported the OECD guidelines, since then it did not implement a law to protect users like in Europe and now lags behind. A key reason being that no "explicit right to privacy" is enshrined in the U.S.

---

[138] *See id.*

[139] Romm, *supra* note 75.

[140] Schinasi, *supra* note 64, at 590.

[141] *Id.*

[142] ZUBOFF, *supra* note 8, at 486–87.

[143] Craig McAllister, *What About Small Businesses? The GDPR and Its Consequences for Small, U.S.-Based Companies*, 12 BROOK. J. CORP. FIN. & COM. L. 187, 189 (2017).

[144] *Id.* at 192.

[145] Dominique-Chantale Alepin, *Social Media, Right to Privacy and the California Consumer Privacy Act*, 29 COMPETITION 96, 107 (2019) (panelist discussion of the GDPR and CCPA).

[146] Barth, *supra* note 112.

Constitution.[147] U.S. business also prefers to be self-regulated.[148] And many of the big tech companies that qualify as surveillance capitalists are U.S. businesses.[149] Of the world's most valuable firms, Apple, Amazon, Alphabet (Google), Microsoft, and Facebook all qualify as internet giants.[150] Policy allowing self-regulation is done out of a belief that such policy and regulation promotes a "customizable and more effective system of protection."[151]

In the United States, the Federal Trade Commission has promoted "self-regulation."[152] Conflicts arise when self-regulation interacts with "sectoral data protection."[153] The problem this approach poses is that "[t]he involvement of state attorneys general, in response to non-enforcement by the FTC, could potentially create discrepancies in privacy policy by state that could greatly hinder business development online."[154] Moreover, an article describing the current enforcement regime in the United States concluded "[i]t is clear that current statutes and regulations are not sufficient to prevent commercial entities from taking advantage of consumers."[155] At one point it looked like the FTC would push for regulation of consumer data, but currently the federal government does not appear ready to take action.[156] Recently, tech companies have begun proposing regulations of certain technologies in what appears to be an attempt to steer the public and users away from regulation of data collection—or surveillance capitalism.[157]

To do business in the EU, U.S. businesses often enter into the Privacy Shield, the successor of the Safe Harbor agreements.[158] This allows businesses and organizations to get "a crash course in EU data protection law."[159] Also in the EU's favor is that "some legal approaches are better candidates for

---

[147] Ryan Moshell, . . . *and Then There Was One: The Outlook for A Self-Regulatory United States Amidst A Global Trend Toward Comprehensive Data Protection*, 37 TEX. TECH L. REV. 357, 373 (2005) (citing Jonathan P. Cody, *Protecting Privacy Over the Internet: Has the Time Come to Abandon Self-Regulation?*, 48 CATH. UNIV. L. REV. 1183, 1193 (1999)).

[148] *Id.* at 374.

[149] These companies include Microsoft, Google, Facebook, Apple to name a few.

[150] RADU, *supra* note 55, at 161.

[151] Moshell, *supra* note 147, at 374.

[152] Schinasi, *supra* note 64, at 585-86.

[153] Moshell, *supra* note 147, at 385.

[154] Schinasi, *supra* note 64, at 584.

[155] Max N. Helveston, *Reining in Commercial Exploitation of Consumer Data*, 123 PENN. ST. L. REV. 667, 701 (2019).

[156] *Id.*

[157] *See generally* Justin Sherman, *Oh Sure, Big Tech Wants Regulation-on Its Own Terms*, WIRED (Jan. 28, 2020)(describing how tech companies like Microsoft, Google, and Facebook are reacting to increased scrutiny and the need for the conversation to be led by the public and not the target of the regulation).

[158] Schwartz, *supra* note 73, at 817.

[159] *Id.*

transplantation than others. Accessible legal models like omnibus data privacy laws are adopted in part due to their ease of enactment and comprehensiveness."[160] This approach makes it easier for European states and other countries across the world to adopt the GDPR.[161]

For these reasons, the current state of the law in the United States is not sustainable and it should follow the EU. "Congress should pass federal data privacy legislation that raises the data privacy and protection standards in the United States, assuages the concerns of foreign nations regarding treatment of personal data in the United States, and ultimately positions the United States to earn an adequacy ruling from the European Commission."[162] Some states, like California, already are or are at least trying to.

C. The California Consumer Privacy Act of 2018 and the inalienable right of privacy in California

Set to go into effect January 1, 2020, the California Consumer Privacy Act (CCPA) will allow users (consumers in the language of the bill) to request what data is being collected and whom it is being shared with by businesses, as well as request that the data be deleted.[163] Echoing William Gibson[164], the CCPA states that "[i]t is almost impossible to apply for a job, raise a child, drive a car, or make an appointment without sharing personal information."[165]

California is taking a position more like that of the EU. Banks are being advised to start taking a more conservative approach to interpretation of the GDPR with "GDPR-esque" laws, such as California's, coming into effect.[166] The Economist presented the similarities and differences most clearly:[167]

Selected Features	CCPA, 2018	GDPR, 2018
Data transparency and access	Yes	Yes
Data deletion	Yes	Yes
Definition of personal information	Broad	Narrow

[160] *Id.* at 818.

[161] *Id.* at 775.

[162] McAllister, *supra* note 143, at 211.

[163] CAL. CIV. CODE § 1798.115 (West 2018).

[164] WILLIAM GIBSON, BURNING CHROME 22 (1986)("We're an information economy. They teach you that in school. What they don't tell you is that it's impossible to move, to live, to operate at any level without leaving traces, bits, seemingly meaningless fragments of personal information."); Barth, *supra* note 112 (describing how this issue can sound like science fiction).

[165] Cal. Assemb. B. 375, 2018 (Cal. 2018), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 (California, at least, has caught up with science fiction and is telling its citizens what we all ought to know).

[166] Lindsay A. Seventko, *GDPR: Navigating Compliance as a United States Bank*, 23 N.C. BANKING INST. 201, 211 (2019).

[167] *Companies Should Take California's New Data-Privacy Law Seriously*, *supra* note 103.

Data portability	All data	Some data
User opt-out from the sale or sharing of data by firms	Easy	Tedious
Right to be forgotten	No	Yes
Maximum fines	Up to $7,500 per individual violation	Up to 4% of global annual revenue, or €20m

California's EU-like data protection will "include an individual's right to know what information a business has collected about them, a right to 'opt out' of allowing a business to sell one's personal information to third parties, a right to deletion, a right to data portability, and a right to receive equal service and pricing from a business, even if one exercises her rights under the Act."[168] In some ways it goes further than the GDPR. For example, its definition of personal information is broader, and Californians must be able to opt out of the sale of their personal data via a "do-not-sell link" which is clearer than the EU process.[169]

In sum, the CCPA "might be certifiable as an adequate privacy protection regime under GDPR Article 45."[170] However, overall, the United States needs regulation that confronts the reality of surveillance capitalism. States' efforts will not likely address all the issues that the mining of users' data raises.[171]

D. Google's reaction

Google, unsurprisingly, does not agree with the decisions against it or any proposal that seeks to constrain its ambition.[172] The decisions against it, and its reaction in the EU, demonstrate this fact.[173]

When the EU Court of Justice granted EU citizens the right to be forgotten, Google was dismissive.[174] When asked about the ruling, Google responded that it plans to collect, analyze, and make available "the world's information" anyway.[175] Sergey Brin wished he and Google could forget about the ruling, and Larry Page suggested Google should be trusted because it cares more about its reputation than the government.[176]

---

[168] Schwartz, *supra* note 73, at 817.

[169] *Companies Should Take California's New Data-Privacy Law Seriously*, *supra* note 103.

[170] J. Thomas Greene, *California and Federal Antitrust Law Update: Procedural Developments*, 29 COMPETITION: J. ANTI., UCL & PRIVACY SEC. CAL. L. ASSOC. 21, 34 (2019).

[171] *See generally* Helveston, *supra* note 155 (identifying the ways in which consumer data in insurance markets is not adequately regulated by state legislatures).

[172] ZUBOFF, *supra* note 8, at 60.

[173] *Id.*

[174] *Id.* at 59.

[175] *Id.* at 60.

[176] *Id.* at 60.

Google may come close to overreaching. When asked, Americans broadly believe they should have control over who gets their information.[177] It is hubris on Google's part to believe that it will unilaterally solve all the world's problems. Or that consumers really want completely personalized search results and ads, delivered by a service that knows and tells you what you want before you even formulate the question.[178]

It is worth noting that article 4 of the GDPR sets forth that "[t]he processing of personal data should be designed to serve mankind."[179] From there it is reasonable to suggest that the burden should be placed on Google to prove that design and not just ask us to take it at its word. Eventually, Congress should not be afraid of backlash for protecting its constituents and establish a national baseline floor of protection like what is found in the EU.

V. CONCLUSION

As the country of origin for surveillance capitalists like Google, the United States owes its citizens a clear right to privacy. A patch work system relying on conflicting state laws, court opinions, self-regulation, and attorney general investigations under the aegis of antitrust will not suffice.[180] A concern is that, under current antitrust law, companies would become smaller but continue to collect data and engage in mass data collection—surveillance capitalism.[181] But subject to mounting weekly criticism, even a captain of surveillance capitalism can long for comprehensive regulation.[182] They may get it too; currently 120 countries have enacted GDPR-like data privacy laws.[183]

Inadvertently, we have let the cameras, microphones, and tracking systems of a dystopia into our homes, and they are wonderful. They may not always be so. The American public perceives that something is not quite right and is beginning to look at tech companies less positively than in recent years.[184] In the midst of an immense economic expansion, of which the tech

---

[177] ZUBOFF, *supra* note 8, at 61.

[178] *Big Other*, *supra* note 31, at 83.

[179] GDPR, *supra* note 5, art. 4.

[180] SCOPE OF U.S. PRIVACY LAW TODAY, 2018 TXCLE-ACCL 1-II, 2018 WL 6687719.

[181] Barth, *supra* note 112.

[182] Peter Kafka, *Mark Zuckerberg Wants You – and Your Government – to Help Him Run Facebook*, VOX (Mar. 31, 2019), https://www.vox.com/2019/3/31/18289375/mark-zuckerberg-facebook-regulation-washington-post-op-ed (discussing Zuckerberg's suggestion that more countries implement the GDPR). *But see* Jason Tashea, *European Union High Court Sends New Signals on Reach of Internet Regulation*, ABA J. (Oct. 10, 2019), https://www.abajournal.com/web/article/eu-high-court-sends-mixed-signals-on-reach-of-internet-regulations (describing Zuckerberg's resolve to continue litigating decisions against Facebook regarding take down requests); Barth, *supra* note 112 ("Before Cambridge Analytica . . . every tech journalist had to write the Facebook privacy piece, like once a year at least. Now it's one a week.") (quoting Antonio Garcia Martinez, tech columnist and former Facebook product manager).

[183] Schwartz, *supra* note 73, at 777.

[184] Carroll Doherty & Jocelyn Kiley, *Americans Have Become Much Less Positive About Tech Companies Impact on the U.S.*, PEW RESEARCH CTR. (July 29, 2019), https://www.pewresea

sector is a huge driver, Americans are criticizing this area more.[185] Logically then, fifty-five percent of Americans think the sector has too much power and influence.[186] Understanding Google through the lens of surveillance capitalism allows legal practitioners to better consider how the law should apply to the rights of users interacting with the marvelous technology at our fingertips.

While the laws proposed in states like California offer a hopeful starting point, there should be a national floor for the protection of our data[187] from this new commodity: behavior. Because this market and concern is global, in the long run, it will not be enough to continue to allow self-regulation or regulation state by state. Citizens of the United States and users all over the world need protections like those put forth in the GDPR. As the United States enters the second decade of the 21st century, it is time for privacy law to catch up with the evolving economy.

Ultimately, the U.S. government should establish the floor for the states, as the EU has for its member countries. But in the United States, this will require an understanding of the nature of Google and similar firms that are in fact surveillance capitalists, and that the users are a means to an end in a new market for behavior.[188] We must all understand that "data" means "people."[189] That data—"the new oil"—is people. That "[a]n information civilization shaped by surveillance capitalism and its new instrumentarian power will thrive at the expense of human nature, especially the hard-won capacities associated with self-determination and moral autonomy that are essential to the very possibility of a democratic society."[190] To that end, the attorneys general conducting this antitrust investigation should hammer this point home wherever and however they conclude their investigation of Google.

---

rch.org/fact-tank/2019/07/29/americans-have-become-much-less-positive-about-tech-companies-impact-on-the-u-s/.

[185] *Id.*

[186] *Id.* (discussing Americans' concerns in this area with tech also extend into social media companies management of political discourse and these companies' inability to determine what is offensive and simultaneous belief that these companies have a responsibility to remove offensive content).

[187] RADU, *supra* note 55, at 157.

[188] ZUBOFF, *supra* note 8.

[189] *How to Think About Data in 2019*, *supra* note 107.

[190] Zuboff, *supra* note 3, at 25.