University of Miami Business Law Review

Volume 28 | Issue 2 Article 9

September 2020

The United States: Big Data, Little Regulation

Megan Valent

THE UNITED STATES: BIG DATA, LITTLE REGULATION

Megan Valent[1]

In the United States today, there is no single law to address the privacy concerns associated with the collection of consumer data. Lawmakers have introduced policies that seek to address data privacy at the federal level, but Congress has not yet acted to create a comprehensive law to protect consumers. On the contrary, in 2016, the European Union passed its General Data Protection Regulation to address the dangers associated with "Big Data" and to give consumers control over their data.

Unfortunately, in the United States consumers are often unaware of how their data is being handled and what is done with their data once a security breach has occurred. In Kaufman v. Google LLC*, for instance, Ronnie Kaufman filed a class action lawsuit against Google for its alleged deceptive practices of tracking and storing location data after users apparently deactivated Google's ability to track and store this data. According to the complaint, Google represented to the public and its users that it would not access user location history if users took certain steps in managing their privacy settings. Unfortunately, however, Kaufman alleged that Google continued to track and store her personal data.*

This note analyzes the implications of the Big Data Era on individual privacy rights in the United States. It argues that companies should write "opt-out" privacy policies in a clear and

[1] Juris Doctor Candidate, University of Miami School of Law (2020); Bachelor of Science, Florida State University (2017). I thank Professor Cheryl Zuckerman for her helpful commentary at different stages of my article and her continuous encouragement. I also thank the editors of the *University of Miami Business Law Review* for their insight and feedback.

comprehensible manner, so that consumers are completely aware of the ways in which personal data is being collected. If used correctly, big data is extremely beneficial to a functional society and to the business world. Yet, to preserve big data's benefits, the United States must stop falling behind in its regulation.

I. INTRODUCTION

It is Christmas, and you sign on to Google to search "best gifts for my kids this Christmas." A ton of search results appear, and the results are tailored exactly to the age-groups of your children. Your children's favorite brands and items similar to what you have recently purchased appear in the search results. You are happy that data mining[2] has made online shopping easier than ever before. But what if you knew that your every move was being tracked by your technological devices every day? Would you knowingly give up privacy for efficiency?

We live in the "Big Data Era"–an era in which companies collect vast amounts of consumer data to work more efficiently and productively. Researchers and decision-makers have realized that big data is beneficial for understanding consumer needs, improving service quality, and predicting and preventing risks.[3] For example, one of the most remarkable

---

[2] *See generally Data mining Definition*, DICTIONARY.COM, https://www.dictionary.com/browse/data-mining (last visited Jan. 7, 2019) ("The process of collecting, searching through, and analyzing a large amount of data in a database, as to discover patterns or relationships.").

[3] Li Cai & Yangyong Zhu, *The Challenges of Data Quality and Data Quality Assessment in the Big Data Era*, DATA SCIENCE J., May 22, 2015, at 2.

stories of the beneficial impacts of big data emerged from Haiti after the 2010 earthquake.[4] Researchers at the Karolinska Institute and Columbia University obtained data on people fleeing Haiti's capital, Port-au-Prince, by tracking approximately 2 million cell-phone SIM cards in the country.[5] In doing so, the researchers were able to pinpoint the location of over approximately 600,000 people affected by the earthquake and made this information available to government and humanitarian organizations.[4] Through their efforts in Haiti, researchers from the Karolinska Institute and Columbia University revealed big data's value and the critical impact it may have on society.[6]

However, for Americans, the Big Data Era has started to raise privacy concerns. These concerns stem from the ever-growing tension between individual privacy rights and the marketing interests of merchants and companies in the United States.[7] With tech-companies recently "under fire" for mishandling user-data,[8] lawmakers are now demanding transparency in company privacy policies and the methods for which vast amounts of consumer data is being collected on a daily basis.

In November 2018, Ronnie Kaufman filed a class action lawsuit against Google LLC ("Google") for Google's alleged deceptive practices of tracking and storing location data after users deactivated the ability to track and store this data.[9] According to the complaint, Google allegedly represented to the public and its users that it would not access user location

---

[4] *See generally* Tom Silva, *The Era of Big Data Is Here*, HUFFINGTON POST, https://www.huffingtonpost.com/tom-silva/the-era-of-big-data-is-he_b_1606914.html (last updated Aug. 18, 2012).

[5] *Id.* ("Later that year, the same team tracked the movements of people during a cholera outbreak allowing aid organizations to mobilize.").

[6] *See also* Gary Marcus & Ernest Davis, *Eight (No, Nine!) Problems With Big Data*, N.Y. TIMES (Apr. 6, 2014), https://www.nytimes.com/2014/04/07/opinion/eight-no-nine-problems-with-big-data.html ("[A]lmost every successful artificial intelligence computer program in the last 20 years, from Google's search engine to the I.B.M. 'Jeopardy!' champion Watson, has involved the substantial crunching of large bodies of data.").

[7] *See generally* Brian Keith Groemminger, *Personal Privacy on the Internet: Should It Be A Cyberspace Entitlement?*, 36 IND. L. REV. 827, 827 (2003).

[8] *See* Laura Litvan, Billy House & Ben Brody, *Facebook Under Fire Over Data Sharing With Chinese Firms*, BLOOMBERG (June 6, 2018), https://www.bloomberg.com/news/articles/2018-06-06/facebook-s-data-sharing-with-chinese- firms-roils-key-lawmakers (explaining how Facebook, Inc. came under fire from U.S. lawmakers in 2018 when it disclosed data-sharing partnerships it had with Chinese consumer-device makers); *see also* Seena Gressin, *The Equifax Data Breach: What to Do*, FED. TRADE COMM'N (Sept. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do (describing the Equifax data breach in 2017 where 143 million American names, Social Security numbers, birth dates, addresses, and driver's license numbers were stolen).

[9] *See* Kaufman v. Google LLC et al., No. 5:18-cv-06685 (N.D. Cal. Nov. 2, 2018).

data if users took certain steps in managing their privacy settings.[10] However, Kaufman argued to the District Court for the Northern District of California that Google's representation was false.[11] In her complaint, Kaufman relied upon an Associated Press investigation's reports, which reported that in 2018 Google accessed and stored the precise geolocation information from individuals who affirmatively disabled Google's "Location History" setting.[12] The investigation results explained that even with the Location History feature disabled, Google's applications still automatically stored time-stamped location data without user consent.[13] Kaufman, an Apple iPhone user, claimed that she attempted to limit Google's ability to track her location by managing the "Location History" setting and turning the Location History storage setting to "off." [13] However, Kaufman alleged that Google continued to track and store her location information.[14]

This Note focuses on the privacy concerns associated with big data and how these concerns impact company liability in the United States. Part II of this Note explains data privacy policies in the United States and how the Federal Trade Commission has attempted to regulate consumer data previously. Additionally, Part II explains how "Online Behavioral Advertising" is regulated in the United States. Part III discusses *Kaufman v. Google LLC* in detail and elaborates on how states have handled location-tracking and data mining. Part IV analyzes the implications on individual privacy rights in the Big Data Era and establishes individual action to minimize the harmful effects of data mining. Lastly, this Note seeks to address the steps companies should take to avoid handling data in an unethical manner, while still being able to achieve productivity and efficiency from the use of big data.

II. DATA PRIVACY IN THE UNITED STATES

When website applications first began collecting data, they seemed "to the average person to be both harmless and helpful."[15] The Internet was a

---

[10] *See id.*
[11] *Id.*
[12] *See* Ryan Nakashima, *AP Exclusive: Google tracks your movements, like it or not,* ASSOCIATED PRESS (Aug. 13, 2018), https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb ("The privacy issue affects some two billion users of devices that run Google's Android operating software and hundreds of millions of worldwide iPhone users who rely on Google for maps or search.").
[13] *See, e.g.*, *id.*
[14] Compl. at 4, Kaufman v. Google LLC et al., No. 5:18-cv-06685 (N.D. Cal. Nov. 2, 2018).
[15] Samantha Radocchia, *Opt-Out Versus Opt-In: How Blockchain Will Change The Data Collection Culture*, FORBES (Oct. 2, 2018), https://www.forbes.com/sites/samantharadocchia/2018/10/02/opt-out-versus-opt-in-how-

place where a person could shop, watch movies, or connect with old friends and classmates. However, as the amount of data that applications collect has been brought to light, public opinion of the Internet has generally shifted.[16] Terms like "data monopoly" and "threat to democracy" are terms that are more frequently being used to discuss the way companies handle consumer data.[17] Yet, in the United States, there is no single, comprehensive federal law to regulate the collection of personal data and address these privacy concerns.[18]

The United States has a patchwork system of data privacy regulations that can sometimes "overlap, dovetail, and contradict one another."[18] Importantly, these guidelines and regulations do not have force of law, but are instead considered "best-practices" for companies that engage in data mining.[19] Nonetheless, there are some federal privacy-related laws that regulate the collection and use of specific types of personal data.[20] For example, federal laws like the Health Insurance Portability and Accountability Act and the Financial Services Modernization Act regulate particular categories of data like personal health and financial information.[21] Similarly, the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act regulate the interception of electronic communications and computer tampering.[22]

A. *Enforcing Data Privacy at the Federal Level Under the FTC Act*

In the United States, online personal information is generally self-regulated, and companies can shape their own consumer privacy practices

---

blockchain-will-change-the-data-collection-culture/#2f4734af1042 ("Part of the problem is that right now, the culture around data sharing is about 'opting out.' When you start using a new app or social media network, checking the box next to 'I have read and agree to the terms' generally puts you in a situation where your data is available to be harvested by the company.").

[16] *See id.*

[17] *See id.*; *see also* Kira Radinsky, *Data Monopolists Like Google Are Threatening the Economy*, HARVARD BUSINESS REVIEW (Mar. 2, 2015), https://hbr.org/2015/03/data-monopolists-like-google-are-threatening-the-economy.

[18] Leuan Jolly, *Data Protection in the United States*, THOMSON REUTERS (Oct. 1, 2018), https://1.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html ?contextData=(sc.Default)&transitionType=Default.

[19] *Id.*

[20] *See id.*

[21] *See id.*; *see also* 42 U.S.C. § 1301 (1997); 15 U.S.C. §§ 6801-6827 (2011).

[22] *See* Jolly, *supra* note 18 (noting that a class action complaint was filed in 2008 that alleged that internet service providers and a targeted advertising company violated these statutes by intercepting data sent between individuals' computers and internet servers); *see also* 18 U.S.C. § 2510 (2002); 18 U.S.C. § 1030 (2018).

on the Internet.[23] However, at the federal level, the Federal Trade Commission ("FTC") is generally responsible for the enforcement and compliance with posted privacy policies in connection to the collection of consumer data.[24] "The FTC is an independent U.S. law enforcement agency charged with protecting consumers and enhancing competition across broad sectors of the economy."[25] The agency has the authority to enforce a wide variety of sector-specific laws, including the Truth in Lending Act, the CAN-SPAM Act, the Children's Online Privacy Protection Act, the Equal Credit Opportunity Act, the Fair Credit Reporting Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act.[26]

"The FTC's primary legal authority comes from Section 5 of the Federal Trade Commission Act."[27] Through Section 5, the FTC has broad authority that allows it to address deceptive trade practices that affect consumers in the United States.[28] Specifically, Section 5 of the Federal Trade Commission Act provides:

> "The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations except banks, savings and loan institutions described in section 57a(f)(3) of this title, Federal credit unions described in section 57a(f)(4) of this title, common carriers subject to the Acts to regulate commerce, air carriers and foreign air carriers subject to part A of subtitle VII of Title 49, and persons, partnerships, or corporations insofar as they are subject to the Packers and Stockyards Act, 1921, as amended [7 U.S.C.A. § 181 et seq.], except as provided in section 406(b) of said Act [7 U.S.C.A. § 227(b)], from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[29]

Furthermore, in addition to Section 5 of the Federal Trade Commission Act, the FTC has implemented a variety of methods to protect

---

[23] Suzanna Shaub, User Privacy and Information Disclosure: The Need for Clarity in "Opt-in" Questions for Consent to Share Personal Information, 5 Shidler J. L. COM. & TECH. 18 (2009) (citing Jane K. Winn & Benjamin Wright, Law of Electronic Commerce § 14.01 (4th ed. ASPEN L. & BUS. 2001 & Supp. 2007)).
[24] *See id.*
[25] FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE: 2017 (2017).
[26] *Id.*
[27] *Id.*
[28] *See id.*
[29] Federal Trade Commission Act § 5, 15 U.S.C. § 45(a) (2018).

consumer privacy.[30] Importantly, the FTC has the authority to bring enforcement actions against entities engaged in law violations and require these entities to remediate unlawful behavior.[31] In doing so, the FTC may require these entities to implement comprehensive privacy and security programs, provide monetary redress to consumers, and delete illegally obtained consumer data and information.[32] Moreover, "[i]f a[n] [entity] violates an FTC order, the FTC can seek monetary penalties for the violations."[33] In 2017, the FTC reported that it brought hundreds of data security cases to protect consumer data.[34]

Over the last several years, the FTC has taken administrative action against several large companies that have breached their promises to safeguard consumer data.[35] The FTC brought enforcement actions against "Google, Facebook, Twitter, and Microsoft, as well as lesser-known companies."[36] The FTC also brought actions against entities that suffered from an inadvertent data breach and against entities that made significant or material changes in privacy policies without notifying users.[37] Importantly, however, consumers are not afforded a private right of action under Section 5 of the FTC Act, and thus these types of actions are rarely brought and often settled.[38] As a result, states have created "Little FTC Acts"[39] that provide individuals with a private right of action at the state level by incorporating Section 5 jurisprudence into statutory regimes.[40]

---

[30] FED. TRADE COMM'N, supra note 25.
[31] *See id.*
[32] *See id.*
[33] *Id.*; *see also* A Brief Overview Of The Federal Trade Commission's Investigative And Law Enforcement Authority, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority (last updated Oct. 2019).
[34] *See* FED. TRADE COMM'N, *supra* note 25.
[35] Shaub, *supra* note 23 (citing Marcia Hofmann, The Federal Trade Commission's Enforcement of Privacy, in PROSKAUER ON PRIVACY (Kristen J. Mathews eds., 2012)).
[36] FED. TRADE COMM'N, *supra* note 25 ("The FTC's consumer privacy enforcement focuses on protecting American consumers, but the orders the FTC obtains in its cases also protect consumers worldwide from unfair or deceptive practices by businesses within the FTC's jurisdiction.").
[37] *See* Shaub, *supra* note 23.
[38] *See id.* ("Because the Act does not expressly provide for a private cause of action, nor has any federal court implied that such an action is available, enforcement actions regarding privacy policy compliance are relatively rare and are often settled."); *see also* Justin J. Hakala, Note, Follow-On State Actions Based on the FTC's Enforcement of Section 5 (Wayne State Univ. Law Sch., Working Paper Grp., Oct. 9, 2008), https://www.ftc.gov/sites/default/files/documents/public_comments/section-5-workshop-537633-00002/537633-00002.pdf.
[39] *See generally* Henry N. Butler and Joshua D. Wright, Are State Consumer Protection Acts Really Little-FTC Acts?, 63 FLA. L. REV. 163, 163 (2011) ("State Consumer Protection Acts (CPAs) were designed to supplement the Federal Trade Commission's (FTC) mission of protecting consumers and are often referred to as 'Little-FTC Acts.'").
[40] See Hakala, supra note 38.

Therefore, entities that fail to comply with their internal privacy policies may ultimately be held liable at both the federal and state level.

B. *The History of Online Behavioral Advertising*

"Online Behavioral Advertising" is defined broadly as the collection of information about a consumer's online activities in order to deliver advertisements targeted to the individual's interest.[41] "The FTC has studied online behavioral advertising since the mid-1990s, when the Internet first emerged as a commercial medium."[42] In doing so, the FTC has conducted workshops, issued reports, and developed basic principles for online behavior advertising.[43] At these workshops, consumers expressed common concerns about data privacy and cross-device tracking on the Internet.[44] Similarly, industry lobbyists expressed a common understanding about the necessary improvements to the self-regulatory regime, but differed on how to implement these regulations.[45] Some lobbyists favored an "opt-out" approach to data collection, while consumer privacy advocates favored an "affirmative consent" or "opt-in" approach.[46]

Nonetheless, the National Advertising Initiative has worked for years to address the need for a comprehensive self-regulatory framework for

---

[41] *See generally* Transcript of Town Hall Record at 8, *Ehavioral Advertising: Tracking, Targeting & Technology* (Nov. 1, 2007), https://www.ftc.gov/sites/default/files/documents/public_events/ehavioral-advertising-tracking-targeting-and-technology/71101wor.pdf.

[42] *See* FED. TRADE COMM'N STAFF REPORT, CROSS-DEVICE TRACKING (Jan. 2017), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf (describing how the FTC has worked to keep pace with the ever-growing technological developments of this era).

[43] *See id.*

[44] *See id.* ("Probabilistic tracking, where consumers are tracked without having signed in to any service, may be particularly surprising and concerning to consumers, especially where sensitive information is involved.").

[45] *See* FED. TRADE COMM'N, STAFF REPORT: CHAPTER II. ONLINE PRIVACY: GENERAL PRACTICES AND CONCERNS (Jan. 10, 2014), https://www.ftc.gov/sites/default/files/documents/reports/staff-report-public-workshop-consumer-privacy-global-information-infrastructure/ftc_staff_report_public_workshop_on_consumer_privacy_on_the_global_information_infrastructure_-_0.pdf.

[46] *See* James V. Corbelli & Stephen L. Korbel, *Jurisdiction, Domain Names, Privacy and Security: How the Digital Age Has Changed Business*, 22 ENERGY & MIN. L. F. 158 (2002) (explaining that an "opt-in" approach requires companies to obtain consumer consent before collecting data, while an "opt-out" approach places the burden on the consumer to inform the sites gathering the information not to share that information with third parties).

online behavioral advertising.[47] Since its inception, the non-profit organization has worked with industry leaders to help develop high standards for online behavioral advertising and the collection and use of consumer data.[48] In 2000, the National Advertising Initiative began to work with leading network advertising agencies, such as 24/7 Media, Engage, and MatchLogic, to create a first-ever framework for self-regulation of the online behavior advertising industry.[49] That year, the National Advertising Initiative made its "groundbreaking" release of "NAI Principles"–a universal set of self-regulatory standards governing online behavioral advertising.[50] As a result, the FTC "unanimously applauded" the National Advertising Initiative for addressing the concerns surrounding the use of consumer data for company advertising and for being the first to require a notice and choice mechanism for consumers.[51] The National Advertising Initiative today has over 100 members—including Google.[52]

Furthermore, the FTC has also attempted to enact privacy legislation in connection to the regulation of online behavioral advertising. As early as 2000, the FTC recommended to Congress that it enact legislation which, together with self-regulatory programs, would ensure protection of consumer privacy online.[53] The recommended legislation would "set forth a basic level of privacy protection for consumer-oriented commercial websites."[54] The FTC suggested such legislation be enacted, because it was worried about the pace at which technology enhanced the capability of online companies to collect, store, transfer, and analyze consumer data.[55] As a result, in 2010, the FTC again proposed legislation to Congress to

---

[47] *See History*, NETWORK ADVERT. INITIATIVE, http://www.networkadvertising.org/about-nai/history/ (last visited Jan. 3, 2019) (describing how the NAI developed based on the "need for a comprehensive self-regulatory framework" for online behavioral advertising).
[48] *See id.* ("NAI is a non-profit organization championing the responsible and transparent use of information for digital advertising.").
[49] *See id.*
[50] *See id.*
[51] *See id.*
[52] *See About The NAI*, NETWORK ADVERT. INITIATIVE, https://www.networkadvertising.org/about-nai/about-nai/ (last visited Feb. 17, 2020); *see also NAI Members*, NETWORK ADVERT. INITIATIVE, https://www.networkadvertising.org/participating-networks/ (last visited Feb. 17, 2020).
[53] *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, A REPORT TO CONGRESS (2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.
[54] *See id.*
[55] *See id.* ("Over the past five years, the Internet has changed dramatically from a large network of computers that touched the lives of few consumers to a new marketplace where millions of consumers shop for information, purchase goods and services, and participate in discussions.").

further address these issues.[56] The "Do No Track" initiative would "let American consumers decide whether to let companies track their online browsing and buying habits."[57] Additionally, the "Do Not Track" mechanism would allow consumers to "opt-out" of data mining through a setting in their browsers, rather than on a site-by-site basis.[58]

Thereafter, in 2011, Senators John Kerry and John McCain introduced similar privacy legislation to Congress.[59] The legislation, called the "Commercial Privacy Bill of Rights Act of 2011", was an Internet privacy bill that aimed to protect sensitive information regarding consumer data.[60] The bill required companies to provide consumers with a "clear, concise and timely notice of privacy practices and of material changes to those practices."[61] Additionally, the bill required that companies "offer a clear and conspicuous mechanism that allow[ed] consumers to opt-out of 'unauthorized uses' of their [personal] information."[62] Importantly, this would mean that consumers would have to give companies affirmative consent in order for their data to be stored and collected online.[63]

Although the 2011 bill has only been introduced to the Senate,[64] another bill with similar goals was introduced to the legislature in 2018.[65] The "Consumer Data Protection Act" was created to "force sweeping

---

[56] *See generally* FEDERAL TRADE COMM'N, PRELIMINARY FTC STAFF REPORT ON PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 63 (2010), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf ("Companies engaged in behavioral advertising may be invisible to most consumers.").

[57] Fred B. Campbell, Jr., *The Slow Death of 'Do Not Track'*, N.Y. TIMES (Dec. 26, 2014), https://www.nytimes.com/2014/12/27/opinion/the-slow-death-of-do-not-track.html.

[58] *Id.*; *see also* Press Release, Fed. Trade Comm'n, FTC Testifies on Do Not Track Legislation (Dec. 2, 2010), https://www.ftc.gov/news-events/press-releases/2010/12/ftc-testifies-do-not-track-legislation ("The Federal Trade Commission told Congress today that while the Commission recognizes that consumers may benefit in certain ways from the practice of tracking consumers online to serve targeted advertising, the agency supports giving consumers a 'Do Not Track' option because the practice is largely invisible to consumers, and they should have a simple, easy way to control it.").

[59] *See* Inside Privacy, *"Commercial Privacy Bill of Rights Act" Introduced in Senate*, COVINGTON & BURLING LLP (Apr. 12, 2011), https://www.insideprivacy.com/data-security/commercial-privacy-bill-of-rights-act-introduced-in-senate/.

[60] *See id.*

[61] *Id.*

[62] *Id.*

[63] *See id.* (noting that the bill would also require companies to also obtain opt-in consent for material changes to stated practices).

[64] *See* Commercial Privacy Bill of Rights Act, S. 799, 112th Cong. (2011).

[65] *See generally* Consumer Data Protection Act, S., 115th Cong. (2018) (discussion draft by Ron Wyden, Sen.).

changes at companies such as Google and Facebook."[66] Under this piece of legislation, consumers would be able to "opt-out" entirely from being tracked on the Internet—similar to the goals of the FTC's 2010 "Do Not Track" initiative.[67] "Relatedly, websites encountering do-not-track users would not be allowed to facilitate third-party collection . . . meaning that ad network code added to websites for the purpose of vacuuming up information about users for third-party companies would essentially no longer be allowed."[68] In support of this bill, Senator Ron Wyden stated, "It's time for some sunshine on this shadowy network of information sharing[.]"[69]

Compared to the United States, the European Union passed the General Data Protection Regulation ("GDPR") in 2016.[70] The GDPR is a regulation that provides "stronger rules on data protection [so that] . . . people have more control over their personal data and businesses benefit from a level playing field."[71] Importantly, the GDPR provides one set of data protection rules for all companies that collect "personal data" in the EU.[72] The regulation defines "personal data" as information related to an "identifiable natural person."[73] Furthermore, under the GDPR, personal

---

[66] *See* Dell Cameron, *Wyden Unveils Plan to Protect Private Data, Restore 'Do Not Track,' and Jail Reckless CEOs*, GIZMODO (Nov. 1, 2018), https://gizmodo.com/wyden-unveils-new-plan-to-protect-private-data-restore-1830153516 ("Companies that violate the standards established by the FTC under the law's authority would also face steep fines, up to 4 percent of their annual revenue."); *see also* Katharine Goodloe & Melanie Ramey, *Wyden Releases Draft Privacy Bill Increasing FTC Authority, Providing for Civil Fines and Criminal Penalties,* COVINGTON & BURLING LLP (Nov. 9, 2018), https://www.insideprivacy.com/data-privacy/wyden-releases-draft-privacy-bill-increasing-ftc-authority-providing-for-civil-fines-and-criminal-penalties/.

[67] *See* Cameron, *supra* note 66.

[68] *Id.*

[69] *Id.*

[70] *See* Matt Burgess, *What is GDPR? The summary guide to GDPR compliance in the UK*, WIRED (Mar. 24, 2020), https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018; *see also* Brian X. Chen, *Getting a Flood of G.D.P.R.-Related Privacy Policy Updates? Read Them*, N.Y. TIMES, (May 23, 2018), https://www.nytimes.com/2018/05/23/technology/personaltech/what-you-should-look-for-europe-data-law.html.

[71] *See EU Data Protection Rules*, EUROPA, https://ec.europa.eu/info/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules/eu-data-protection-rules_en#library (last visited Apr. 10, 2020) ("As of May 2018, with entry into application of the EU General Data Protection Regulation, there is one set of data protection rules for all companies operating in the EU, wherever they are based.").

[72] *See* General Data Protection Regulation, 2018 O.J. (L 119) ("[A]n identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.").

[73] *See id.*

data must be: (1) processed lawfully, fairly, and in a transparent manner; (2) collected for a specified, explicit and legitimate purpose; (3) adequate and limited to what is necessary in relation to the purposes for which the data is processed; (4) accurate and kept up to date; (5) kept only as long as necessary; and (6) processed in a manner that ensures security of the data.[74] The "controller" of the personal data is legally responsible for ensuring that it is in compliance with the GDPR.[75] The GDPR, furthermore, "requires that the terms and conditions [of a website] be written in plain, understandable language, not legalese."[76] Ultimately, a company can be fined up to four percent of its global revenue if the company violates the GDPR's rules and regulations.[77]

III. ENFORCING DATA PRIVACY AT THE STATE LEVEL

Unfortunately, in the United States, technology has developed much faster than the laws that regulate its use.[78] As a result, many states have enacted some form of legislation aimed at addressing the privacy concerns connected to data mining on the web.[79] For example, California "leads the way in the privacy arena, having enacted multiple privacy laws, some of which have far-reaching effects at a national level."[80] Specifically, California Penal Code 637.7 ("CIPA") is a law that regulates data mining and location tracking in California.[81] It provides that "no person or entity

---

[74] *See id.*

[75] *See id.* ("'[C]ontroller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law[.]").

[76] Adam Satariano, *What the G.D.R.P., Europe's Tough New Data Law, Means for You*, N.Y. TIMES (May 6, 2018), https://www.nytimes.com/2018/05/06/technology/gdpr-european-privacy-law.html. This is an important mechanism of the GDPR, as many consumers do not typically understand what the legalese contained in website privacy policies when browsing the web.

[77] *See id.* (noting that a fine of four percent of global revenue is approximately $1.6 billion for Facebook).

[78] *See* Wilson Elser, *iSpy: tracking employees with GPS technology on mobile devices*, JDSUPRA (Nov. 11, 2014), https://www.jdsupra.com/legalnews/ispy-tracking-employees-with-gps-techno-05683/.

[79] *See* Jolly, *supra* note 18.

[80] *Id.*

[81] *See generally* CAL. PENAL CODE § 637.7 (1999) (noting that "'electronic tracking device' means any device attached to a vehicle or other movable thing that reveals its location or movement by the transmission of electronic signals.").

. . . shall use an electronic tracking device to determine the location or movement of a person."[82] The law further provides:

> "[A]dvances in science and technology have led to the development of new devices and techniques . . . the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society."[83]

Importantly, the statute does not apply to a consumer who affirmatively consents to the use of an electronic tracking device.[84] For example, in *Gonzales v. Uber*, Plaintiff Michael Gonzales alleged that Defendant Uber Technologies, Inc. ("Uber") was tracking and storing his location without his consent in violation of Section 637.7.[85] However, the United States District Court for the Northern District of California dismissed the case because Gonzales affirmatively consented to the tracking of his vehicle through his cellphone when he signed up to be a driver for Uber.[86]

Furthermore, like California, Florida has its own "Little FTC Act"[87] called the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA").[88] Under FDUTPA, a violation may be based on "[a]ny rule . . . [or] regulation . . . which proscribes unfair methods of competition, or unfair, deceptive, or unconscionable acts or practices."[89] The statute further provides that "due consideration and great weight" is given to interpretations by the federal courts and the FTC to determine what constitutes deception.[90] FDUTPA is "extremely broad" and is designed to protect the consuming public from entities or individuals that engage in deceptive or unfair trade practices in Florida.[91]

---

[82] *Id.*
[83] *Id.* at § 630.
[84] *See generally id.*
[85] *See* Gonzales v. Uber Techs., Inc., 305 F. Supp. 3d 1078, 1089 (N.D. Cal. 2018), *recons.*, No. 17-CV-02264-JSC, 2018 WL 3068248 (N.D. Cal. 2018).
[86] *See id.*
[87] *See* Hakala, *supra* note 39 ("A Little FTC Act is a state act that tracks the language of FTC Act §5 (15 U.S.C. §45) and serves as a basis for state level antitrust and/or consumer protection actions. State act features, like treble or punitive damages, class actions, private rights of action, and FTC deference, vary widely.").
[88] *See* Fla. Stat. § 501.201 (2019).
[89] *See* Fla. Stat. § 501.203(3) (2019).
[90] *See* Fla. Stat. § 501.204(2) (2019)
[91] *See generally* Pincus v. Speedpay, Inc., 161 F. Supp. 3d 1150 (S.D. Fla. 2015) (citing Day v. Le-Jo Enterprises, Inc., 521 So.2d 175, 178 (Fla. 3d DCA 1988)).

Accordingly, both the FTC Act[92] at the federal level and the "Little FTC Acts" at the state level have attempted to regulate online behavioral advertising, data mining, and location tracking. In 2011, for instance, Google, Inc. agreed to settle FTC charges against it, which alleged that Google, Inc. violated the FTC Act and used deceptive tactics when it launched Google Buzz in 2010.[93] Then, in 2012, the FTC charged Google, Inc. for violating the 2011 settlement agreement.[94] In its complaint, the FTC charged that for several months in 2011 and 2012, Google placed a certain advertising tracking cookie on the computers of Safari users who visited sites within Google's DoubleClick advertising network, although Google had previously told these users they would automatically be opted out of such tracking . . . ."[95] As a result, Google, Inc. paid a record $22.5 million civil penalty to settle the FTC charges against it.[96] Perhaps justifying the record-setting penalty, the FTC reported that "Google, the developer of the world's most popular Internet search engine, generates billions of dollars in revenue annually from selling online advertising services."[97] FTC Chairman Jon Leibowitz went on to state the agency's firm stance that "[n]o matter how big or small, all companies must abide by FTC orders against them and keep their privacy promises to consumers, or they will end up paying many times what it would have cost to comply in the first place."[98]

IV. *KAUFMAN V. GOOGLE LLC*

In 2018, the Associated Press reported (the "AP Report") that certain Google services used on Android and iPhone devices stored consumer

---

[92] *See generally* Federal Trade Commission Act § 5, 15 U.S.C. § 45(a) (2018).

[93] *See* Press Release, Federal Trade Comm'n, FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network (Mar. 30, 2011), https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz ("The proposed settlement bars the company from future privacy misrepresentations, requires it to implement a comprehensive privacy program, and calls for regular, independent privacy audits for the next 20 years.").

[94] *See* Press Release, Federal Trade Comm'n, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

[95] *See id.* ("Cookies are small pieces of computer text that are used to collect information from computers and can be used to serve targeted ads to consumers. By placing a tracking cookie on a user's computer, an advertising network can collect information about the user's web-browsing activities and use that information to serve online ads targeted to the user's interests or for other purposes.").

[96] *See id.*

[97] *See id.*

[98] *See id.*

location data without the affirmative consent of its users.[99] This privacy issue allegedly affected approximately two billion users of devices that used Google's Android operating system and millions of iPhone users that used Google Maps or its search engine.[100] The Associated Press learned of these issues from K. Shankari, a graduate researcher at University of California, Berkeley, and it confirmed its findings with computer-science researchers at Princeton University.[101] Shankari "noticed that her Android phone prompted her to rate a shopping trip to Kohl's, even though she had turned Location History off."[102] Google communicated that the issue was solved; however, it was reported that Google continued tracking users even after Location History settings were turned off.[103]

Similarly, Ronnie Kaufman claimed that she turned off the Location History setting on her iPhone, so that her every move would not be tracked on a daily basis.[104] In her complaint, Kaufman alleged that she affirmatively turned the Location History storage option to "off," which made her believe she was opting-out of Google's practices of collecting and processing information about her daily whereabouts.[105] Yet, unbeknownst to Kaufman, Google allegedly continued to track and store her location information.[106]

As a result, in November 2018, Kaufman filed a class action suit in the United States District Court for the Northern District of California against Google where she claimed that Google's practice of tracking and storing location data after users "opted-out" of the Location History setting was deceptive.[103] In doing so, Kaufman alleged that Google's actions violated CIPA and FDUTPA and constituted intentional and negligent misrepresentation.[107] Furthermore, Kaufman expressed in the complaint that Google represented to the public that it would not access users' location history if the users took certain steps in managing their privacy settings.[108] Essentially, if users disabled the "Location History" feature on

---

[99] *See* Nakashima, *supra* note 12. Plaintiff Ronnie Kaufman used this *AP Exclusive* investigation in her complaint against Google to allege that Google continued to store Kaufman's location and Class Members' location.
[100] *See id.*
[101] *See id.*
[102] *See id.*
[103] *See id.*
[104] Compl. at 4, Kaufman v. Google LLC et al., No. 5:18-cv-06685 (N.D. Cal. Nov. 2, 2018) (arguing that Kaufman attempted to limit Google's ability to use location tracking by managing the Location History settings on Google's website).
[105] *See id.*
[106] *See id.*
[107] *See id.* at 4.
[108] *See id.* at 2.

in their Google accounts, then Google would be prevented from tracking and storing location data.[109]

Kaufman used studies from the AP Report, confirmed by computer-science researchers at Princeton University, to assert that Google accessed and stored precise geolocation information from individuals who affirmatively disabled the Location History setting.[108] The AP Report claimed that "Google stores a snapshot of where you are when you merely open its Maps app . . . [a]nd some searches that have nothing to do with location, like 'chocolate chip cookies,' or 'kids[']science kits,' pinpoint your precise latitude and longitude—accurate to the square foot—and save it to your Google account."[110] The important inference to take away from the AP Report is that it was alleged that Google unlawfully used location tracking information from its users for marketing and advertising purposes in an effort to generate revenues.[110]

Nevertheless, the AP Report also revealed that users could view the stored location markers on a page in Google's website.[111] "To demonstrate how powerful these [location] markers are, the AP created a visual map of the movements of Princeton University postdoctoral researcher Gunes Acar, who carried an Android phone with Location history off and shared a record of his Google account."[112] The map showed all of Acar's movements—his train commute, visits to the "High Line park, Chelsea Market, Central Park and Harlem."[113] Armed with this information, Kaufman alleged that by tracking the locations of users, despite having affirmatively turned off the Location History storage option, Google intruded into the "solitude, seclusion, and private affairs" of each user.[114]

According to the Associated Press, days after the AP Report findings were published, Google announced that it was "updating the explanatory language about Location History to make it more consistent and clear across . . . platforms and help centers."[115] The Associated Press reported that this statement was contradictory, as Google had previously reported that its website descriptions explained the "opt-out"

---

[109] *See id.*; *see also* Nakashima, *supra* note 12.
[110] *See* Compl. at 2, Kaufman v. Google LLC et al., No. 5:18-cv-06685 (N.D. Cal. Nov. 2, 2018); *see also* Nakashima, *supra* note 12.
[111] *See generally* Nakashima, *supra* note 12.
[112] *See id.*
[113] *Id.*
[114] Compl. at 4, Kaufman v. Google LLC et al., No. 5:18-cv-06685 (N.D. Cal. Nov. 2, 2018).
[115] *See* Ryan Nakashima, *Google clarifies location-tracking policy*, ASSOCIATED PRESS (Aug. 16, 2018), https://www.cbsnews.com/news/google-clarifies-its-location-tracking-policy-2018-08-16/.

process for location tracking clearly.[116] Nevertheless, the updated language on Google's website acknowledged that a user's location could still be tracked even if that user "opts-out" of Location History on Google's Website.[116] According to the Associated Press, Google's website was revised to state, "[t]his . . . setting does not affect other location services on your device."[117]

V. ANALYSIS

A. *The "Big Data" Era*

Big data affects our everyday lives. If you use the "Maps" application on your iPhone, google simple questions, or even input daily "caloric intake" on a health application, your data is being collected and big data affects you. Even the FTC acknowledges that, "[w]ith a smartphone now in nearly every pocket, a computer in nearly every household, and an ever-increasing number of Internet-connected devices in the marketplace, the amount of consumer data flowing throughout the economy continues to increase rapidly."[118] Unfortunately, however, the collection of consumer data has been a growing concern for many years,[119] but it is only recently being taken seriously by lawmakers in Congress.

If consumer data is properly secured and companies are completely honest about the ways in which the consumer data is being used, then consumers would not worry about how data is collected and handled. But this is not reality. For instance, in 2017, the Equifax data breach exposed 143 million Americans' personal information.[120] Then, in 2018, it was

---

[116] *See id.* ("[I]ts help page for the Location History setting . . . states: 'This setting does not affect other location services on your device.' It also acknowledges that 'some location data may be saved as part of your activity on other services, like Search and Maps.'").

[117] *See id.*

[118] Fed. Trade Comm'n, Big Data: A Tool for Inclusion or Exclusion? (Jan. 2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf ("Companies have been analyzing data from their own customer interactions on a smaller scale for many years, but the era of big data is still in its infancy.").

[119] Network Advert. Initiative, *supra* note 47 ("Since 2000, [the Network Advertising Initiative] has worked with leaders in the online advertising industry to help develop high standards for online behavioral advertising and to provide consumers with the ability to exercise choice.").

[120] Seena Gressin, *The Equifax Data Breach: What to Do*, Fed. Trade Comm'n (Sept. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do; *see also U.S. and World Population Clock*, United States Census Bureau https://www.census.gov/popclock/ (last updated Jan. 9, 2019) (noting that the American population consists of approximately 300 million people, and therefore over half of the U.S. population was affected by the Equifax data breach).

discovered that Cambridge Analytica gained access to the data of nearly "50 million Facebook users as a way to identify the personalities of American voters and influence their behavior."[121] Consumers may seek to file a claim against these large tech-companies; however, they are left in the dark as to what is done with their personal data after a breach has occurred.

Nevertheless, there is an ever-growing tension between individual privacy rights and convenience.[122] On the one hand, the amount of data that companies store and collect for each technology-using individual is frightening.[123] Even if an individual's Google Location History is turned off, a smartphone's location can still be tracked daily.[124] And unfortunately, if companies do not adequately protect the data they collect, consumers may fall victim to data breaches. On the other hand, the collection of big data has made life easier. Online shopping has become more efficient, since advertisements and sales are now narrowly tailored towards each individual shopper's liking. As one *Forbes* article articulates, "[B]ig Data can [also] be harnessed to help address social problems of hunger, disease, poverty, and social inequity."[125] Regardless of whether a consumer values their privacy or data efficiency more, big data is here to stay. Thus, United States lawmakers should start paying attention to the issues involved in the collection of big data and to the benefits it may bring to various aspects of consumer life if handled in a more secure way.

---

[121] *See generally* Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. Times (March 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

[122] *See generally* Adam Satariano, *What the G.D.R.P., Europe's Tough New Data Law, Means for You*, N.Y. Times (May 6, 2018), https://www.nytimes.com/2018/05/06/technology/gdpr-european-privacy-law.html ("The internet's grand bargain has long been trading privacy for convenience. Businesses offer free services like email, entertainment and search, and in return they collect data and sell advertising.").

[123] However, even if an individual is not using technology per se—his or her information may still be collected by tech-companies who collect data. *See generally* Edward C. Baig, *How Facebook can have your data even if you're not on Facebook*, USA Today (Apr. 13, 2018), https://www.usatoday.com/story/tech/columnist/baig/2018/04/13/how-facebook-can-have-your-data-even-if-youre-not-facebook/512674002/ ("One of the creepiest things brought to light during Mark Zuckerberg's testimony on Capitol Hill this week was how Facebook can amass data to construct what are being referred to as 'shadow profiles' of you, even if you've never opted in or joined the world's largest social network.").

[124] *See generally* Nakashima, *supra* note 12.

[125] *See generally* Randy Bean, *Another Side of Big Data: Big Data For Social Good*, Forbes (Sep. 23, 2016), https://www.forbes.com/sites/ciocentral/2016/09/23/another-side-of-big-data-big-data-for-social-good/#2f096c423033.

B. Kaufman v. Google LLC *and More on "Online Behavioral Advertising"*

If the allegations explained in the complaint are in fact true, Kaufman did what a consumer who valued their privacy rights would do. Kaufman owned an Apple iPhone that had various Google applications and functionalities downloaded onto it.[126] She allegedly "attempted to limit Google's ability to track her location by managing her Location History settings on Google's website."[127] She turned the Location History storage option "off", but that still was not enough.[128] Despite taking these actions, Kaufman claimed that Google continued to track and store her location data and information.

Unsurprisingly, however, Google was fined $57 million dollars under the GDPR recently in January 2019.[129] The French data protection authority announced that it fined Google for "not properly disclosing to users how data is collected across its services—including its search engine, Google Maps and YouTube—to present personalized advertisements."[130] Similarly, in 2012 Google, Inc. was forced to "pay a record $22.5 million civil penalty to settle [FTC] charges that it misrepresented to users of Apple Inc.'s Safari Internet browser that it would not place tracking 'cookies' or serve targeted ads to those users . . . ."[131] In its complaint, the FTC charged that for several months in 2011 and 2012, Google placed "a certain advertising tracking cookie on the computers of Safari users who visited sites within Google's DoubleClick advertising network, although Google had previously told these users they would automatically be opted out of such tracking . . . ."[132] Likewise, in *Kaufman v. Google LLC*, Google allegedly misrepresented to the public that if users turned the Location History storage option "off" on their cellular devices, Google would no longer track each individuals location history.[133]

---

[126] *See* Compl. at 4, Kaufman v. Google LLC et al, No. 4:18-CV-06685 (N.D. Cal. Nov. 2, 2018) (noting that at the time of the Complaint, Kaufman used an iPhone X and had owned and used an iPhone 7 before then).

[127] *See id.*

[128] *See id.* (noting that Kaufman claimed she believed that by affirmatively turning the Location History storage option to "off", she was opting out of Google's practices of collecting and processing information about her actual location).

[129] *See generally* Adam Satariano, *Google Is Fined $57 Million Under Europe's Data Privacy Law*, N.Y. TIMES (Jan. 21, 2019), https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html.

[130] *Id.*

[131] *See* Press Release, *supra* note 94.

[132] *Id.*

[133] *See* Kaufman v. Google LLC et al, No. 4:18-CV-06685 (N.D. Cal. Nov. 2, 2018).

Companies like Google must develop a more transparent way to safely collect consumer data. American consumers may not be aware of the fact that certain applications track location data on a daily basis. For those who are aware, like Kaufman, there are usually ways to "opt-out" of location tracking. However, the "opt-out" process must be comprehensible to consumers. As Kaufman alleged in her complaint against Google, the AP Report revealed that even when consumers "opt-out" of Location History tracking, "Google store[d] user location when, for instance, the Google Maps app is opened, or when users conduct Google searches that aren't related to location.[134]

Moreover, it is best for companies that are engaged in online behavioral advertising and the collection of consumer data to lay out "opt-in" and "opt-out" policies in a clear and comprehensible manner for consumers.[135] Many times, it is difficult for a consumer to understand or decipher the terms of a contract. This is because companies may use "legalese" to hide the terms of the contract to their benefit. It is also essential for companies engaged in online behavioral advertising to be honest about the ways in which consumer data is collected. This may seem like common sense, but shockingly enough consumers are still often left in the dark as to what is happening to their data being collected on the Internet.[136] Company privacy policies and notices in the United States should clearly and honestly advise each consumer as to what is being done with their data and why it is being collected and stored to begin with.[137]

In addition to laying out privacy policies in a clear and comprehensible manner, companies should consider an "opt-in" approach to avoid any confusion or misrepresentation. To "opt-in" means to "to choose to be involved in or part of a scheme," while "opt-out" means "to decide to leave

---

[134] *See generally* Nakashima, *supra* note 114.

[135] *See* Andrew Rossow, *The Birth Of GDPR: What is it and What you Need to Know*, FORBES (May 25, 2018), https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/#78ec7ff255e5; *see also* Cara Johnson, *What's in a notice? Privacy notices under the GDPR*, PRIVACY & DATA SECURITY INSIGHT (Feb. 28, 2018), https://www.privacyanddatasecurityinsight.com/2018/02/whats-in-a-notice-privacy-notices-under-the-gdpr/ (noting that unlike the U.S., the EU's GDPR requires that the use of personal data must be "'fair and lawful'— in other words, individuals must receive clear and transparent notice of both (1) the ways in which, and (2) the purposes for which their data will be used.").

[136] *See generally* Steve Olenski, *For Consumers, Data is a Matter of Trust*, FORBES (Apr. 18, 2016 9:35 AM), https://www.forbes.com/sites/steveolenski/2016/04/18/for-consumers-data-is-a-matter-of-trust/#552636e978b3 (explaining how, according to research, consumers like to know how their information is being shared).

[137] This is similar to what the GDPR requires of companies in the EU.

or withdraw."[138] In the United States, the National Advertising Initiative offers "opt-out" tools to assist consumers in making choices as to the participating companies that use cookies for "Interest- Based Advertising" and "Cross-App Advertising."[139] Under this scheme, American consumers are automatically included in online behavioral advertising, unless they affirmatively request to "opt-out" of the agreement. An "opt-in" approach, however, would require companies engaged in these advertising mechanisms to obtain consent prior to collecting vast amounts of consumer data.[140] Thus, if the United States adopted an "opt-in" affirmative consent approach, similar to the EU's GDPR standard for data collection, Google would have been forced to obtain consent from Kaufman before it stored her location data. Yet, this was not the case, and Kaufman therefore allegedly decided to "opt-out" of Google's location tracking after it was already too late. Altogether, because the United States has followed an "opt-out" approach for so many years, vast amounts of consumer data has already been collected and thus we now have the Big Data Era.

Overall, the United States should move towards passing legislation aimed at regulating the collection of big data. Although it is too soon to assess the effectiveness of the GDPR in the EU, a company like Google that is charged $57 million for violating the GDPR will no doubt change the way big data is handled to gain legal compliance. For instance, companies that are fined under the GDPR will be more motivated to make sure that privacy policies are in compliance with the GDPR's regulations in order to avoid more fines. Furthermore, if the United States created a comprehensive data protection law at the federal level, consumers who are misrepresented as to the way data is collected and handled would be able to bring a federal claim rather than a state claim against these companies that did so. Today, however, plaintiffs like Kaufman must assert these claims in state court, where dockets are overcrowded, and hundreds of other cases are waiting to be heard. In the meantime, plaintiffs like Kaufman are left to wonder how their data is being handled while they are waiting for these lawsuits to be heard. Furthermore, data breaches have

---

[138] *See Opt-out Definition*, DICTIONARY.COM, https://www.dictionary.com/browse/opt-in (last visited Jan. 10, 2019); *see also Opt-in Definition*, DICTIONARY.COM, https://www.dictionary.com/browse/opt-in (last visited Jan. 10, 2019).

[139] *See generally Understanding Online Advertising*, NETWORK ADVERT. INITIATIVE (last visited Jan. 26, 2020), https://www.networkadvertising.org/understanding-online-advertising/what-are-my-options/.

[140] *But see* Daniel Castro, *How an "Opt-In" Privacy Regime Would Undermine the Internet Ecosystem*, INFO. TECH. & INNOVATION FOUND. (May 26, 2017), https://itif.org/publications/2017/05/26/how-opt-in-privacy-regime-would-undermine-internet-ecosystem ("Forcing companies to obtain affirmative consent to collect and use certain user data would raise their costs and leave them with a few bad options to adapt.").

become a normal occurrence in the twenty-first century, and consumers must be able to feel at ease with the way data is being collected, used, and stored by American companies.

VI. CONCLUSION

Thomas H. Davenport once said, "[e]very company has big data in its future and every company will eventually be in the data business." Well, that future is now, and it has a major impact on consumers. It is crucial that companies involved in the collection of consumer data and online behavioral advertising be as fair as possible in explaining how consumer data is being handled and what is being done with consumer data. Simultaneous responsibility falls on consumers to start paying attention to privacy notices and to what is being done with their data. In *Kaufman v. Google LLC*, Kaufman was a consumer who became aware of the ways in which Google was collecting her data and tried to "opt-out" of the practice. Yet, that apparently did not work. It will be interesting to see how the Northern District Court of California handles this case and to see how the United States Congress plans to finally regulate the way consumer data is collected today. If used correctly, big data is extremely beneficial to a functional society. To preserve big data's benefits, the United States must stop falling behind in its regulation.