University of Miami Business Law Review

Volume 30 | Issue 3 Article 7

Investing in Human Futures: How Big Tech and Social Media Giants Abuse Privacy and Manipulate Consumerism

Brett Dembrow

Investing in Human Futures: How Big Tech and Social Media Giants Abuse Privacy and Manipulate Consumerism

BRETT DEMBROW

Abstract

Social media companies such as Facebook, Twitter, and Instagram originated with one seemingly innocent goal: "to bring the world closer together."[1] *Now, these Big Tech giants own and operate some of the most powerful platforms in the world simply because of their unethical yet effective strategies to maintain their users' attention. Social media companies have monetized the amount of time their users spend on their platforms by honing in on the individual preferences of each user and selling that access to advertisers. This heightened access to potential consumers and their preferences has become the most valuable marketing tool for digital advertisers. However, this increased access has led to increased public distrust in Big Tech companies and their practices. This public sentiment has resulted in stringent proposed state and federal legislation, as well as self–regulation. Legislatures and corporations alike acknowledge that change is necessary, but neither side has agreed on where to draw the line. This comment examines the privacy implications of the targeted advertising business model and practices, the legal and legislative challenges Big Tech companies have faced, and a potential solution to the exploitation of user data.*

---

1 *See* Josh Constantine, *Facebook changes mission statement to 'bring the world closer together'*, TECH CRUNCH (June 22, 2017), https://techcrunch.com/2017/06/22/bring–the–world–closer–together/.

I. INTRODUCTION

After a family vacation in Madrid, you post your favorite photos on Facebook and tag the location of the various sites you visited. The following week, you notice that Madrid hotel and Airbnb advertisements have filled your Facebook, Twitter, and Instagram feeds. While it may seem like these platforms are clairvoyant, the reality of the situation proves to be much more dubious. Although social media companies do not charge their users a dollar amount in exchange for use of their platforms, they collect something much more valuable: personal data and information.

Upon creating a Facebook account, users immediately agree to the company's terms and conditions.[2] These terms, coupled with Facebook's privacy policy, grant the company the ability to collect the user's data, bundle the user's data with that of similar users, and sell the bundled consumer information to applicable advertisers.[3] In this age of "instant

---

[2] *See* Sophie Gallagher & Max Thurlow, *These Are All The Facebook Terms And Conditions You Agreed To When You Opened An Account*, THE HUFFINGTON POST (Mar. 26, 2018), https://www.huffingtonpost.co.uk/entry/facebook–terms–and–conditions–you–agreed–to–when–you–opened–an–account–what–do–they–mean_uk_5ab8b719e4b054d118e47db9

[3] *Id*.

gratification" and information overload, social media users eagerly share their information with other users in their network. What users may not fully understand is that while they indeed share information about last night's Miami Spice meal with their friends in a tweet, they also share that information indirectly with advertisers. Actually, every interaction a user has on social media, whether it's posting a status, retweeting a news article, or posting an Instagram story, provides advertisers with more information to monetize.

Although not explicitly mentioned in the Constitution, Americans rely on a reasonable expectation of privacy as they go about their personal and daily lives.[4] The Fourth Amendment alludes to some of these protections, but the Founding Fathers never could have imagined data collection algorithms and machines gaining access to the information of hundreds of millions of people.[5] Privacy continues to be a grey area in legal doctrine and personal liberties, and although Congress has passed laws to protect consumer information, the protections have not gone far enough.

Social media companies argue that by agreeing to their terms and conditions and privacy policies, users relinquish their expectation of privacy while using the platform and its associated services. These Big Tech giants have become some of the wealthiest companies in the history of the world in less than two decades.[6] By providing users with access to social media platforms without a monetary cost, social media companies knew they needed to generate revenue to continue fueling their users' addiction. This paved the way for the targeted advertising model to dominate social media platforms in a quick and precise fashion.

Websites should have a privacy policy that explains to its users what information is collected, how it is used, how it may be shared, and how it is secured. In order to be fully compliant with American and European data protection laws, all data subjects should have the opportunity to consent to the collection of personal information. While users volunteer much of their information when they sign up for newsletters, complete forms, or send email requests, information gathered from third parties and through the use of cookies should also be disclosed. Users should be given the opportunity to consent to, block, or disable cookies.

---

4 *See* Charlie Warzel, *Facebook Under Oath: You Have No Expectation of Privacy*, THE NEW YORK TIMES (June 18, 2019), https://www.nytimes.com/2019/06/18/opinion/facebook–court–privacy.html.

5 *See* Florencio Travieso, *The Legal Implications of Digital Privacy*, GOVERNMENT TECHNOLOGY (Jan. 15, 2019), https://www.govtech.com/public–safety/The–Legal–Implications–of–Digital–Privacy.html.

6 *See* Irena Martinčević, *Visualizing Top 20 Most Valuable Companies of All Time*, HOW MUCH (Dec. 23, 2019), https://howmuch.net/articles/the–worlds–biggest–companies–in–history.

Part II of this comment will analyze the targeted advertising business model and how social media companies generate revenue by selling user data. Part III will address the legislative attempts to halt social media companies' data collection and privacy infringement practices. Part IV of this comment proposes three solutions: a data tax, which would give social media companies a choice as to whether or not they wish to continue these practices; expanding California's data privacy laws nationally; or self–regulation through top–down leadership. Part V will address the outcomes of these proposed solutions and the role they play on reining in the power and influence of Big Tech companies.

II. TARGETED ADVERTISING BUSINESS MODELS

As of 2019, Facebook's targeted advertising business model produced over $70 billion in revenue and $8 billion in net income, while the company boasts 2.5 billion users globally.[7] The global social media platform sells advertising to businesses that use the data Facebook collects on users to target ads.[8] Facebook advertising revenues accounted for 98.52% of total revenue in 2019, highlighting the focus of their revenue strategy.[9] The U.S. and Canada still are the dominant geography for ad revenue, accounting for 48.6% of total revenue in 2019.[10] How long a user spends on a social media platform determines their value to an advertiser. If a user spends more time, shares more content, and posts more updates on their Facebook account, they will likely carry more value to an advertiser than someone who uses Facebook once per week.

In essence, Facebook's business model charges advertisers for access to precisely targeted segments of their massive consumer database. For example, if a user searched for Trader Joes' Facebook page and liked some of the posts on the page pertaining to Fall Specials and pumpkins, Facebook would receive information about that user.[11] Facebook's algorithms would then put that user in the 'fall seasonal' target segment, the 'Trader Joes' target segment, and the 'grocery store' target segment. Advertisers for a local pumpkin patch, Trader Joe's, and Whole Foods would then approach Facebook and purchase the target segments that directly correlate with the product or service they want to sell. In the

---

7 Gary Fox, *Facebook Business Model: How Does Facebook Make Money*, GARY FOX (Mar. 8, 2020), https://www.garyfox.co/facebook–business–model–makes–money/.

8 *Id.*

9 *Id.*

10 *Id.* at 5.

11 *See* Paige Bennett, *18 of the best seasonal fall foods to buy at Trader Joe's right now*, INSIDER (Sept. 14, 2020), https://www.insider.com/seasonal–fall–foods–at–trader–joes–2018–9.

coming days and weeks, that user will likely see advertisements from these companies because of their prior search history and interactions on Facebook.

Facebook does not use Wi–Fi data to determine a users' location for ads if the user has Location Services turned off, but it does use IP and other pertinent location–specific information such as relating to the user's posts or location tags.[12] In doing this, Facebook can collect data on what stores or shops the user has visited and what type of areas the user enjoys spending their time.

In 2017, Facebook's average revenue per user (ARPU) in North America was $84.41.[13] A recent study shows that 77% of Facebook user–respondents would continue using the social media platform with its current advertisements and marketing strategies, while 23% would rather opt in to an advertisement free version of the social media site which would come with a monthly fee.[14] Nearly 42 percent said they'd spend between $1 and $5 a month for Facebook.[15] About 25 percent said they'd pay between $6 and $10—or what Facebook is already—making per user.[16]

In 2018, the Pew Research Center conducted a study on how consumers believe Facebook categorizes user data.[17] Through Facebook's "Your ad preferences" page, the site allows users to see how the company's algorithm has categorized their interests and preferences on a variety of issues. Overall, 74% of Facebook users say they had no idea that the company recorded this data until they reached the part of the study that referenced such data.[18] When directed to the "ad preferences" page, the large majority of Facebook users (88%) found that the site had generated some material for them.[19] A majority of users (59%) say these categories reflect their real–life interests, while 27% say they are not very or not at all accurate in describing them. Once shown how the platform classifies

---

12 *See* Kashmir Hill, *Turning Off Facebook Location Tracking Doesn't Stop It From Tracking Your Location*, GIZMODO (Dec. 18, 2018), https://gizmodo.com/turning–off–facebook–location–tracking–doesnt–stop–it–f–1831149148.

13 Len Sherman, *Why Facebook Will Never Change Its Business Model*, FORBES (Apr. 16, 2018), https://www.forbes.com/sites/lensherman/2018/04/16/why–facebook–will–never–change–its–business–model/?sh=93fc03464a7a.

14 Rani Molla, *How much would you pay for Facebook without ads?*, VOX (Apr. 11, 2018), https://www.vox.com/2018/4/11/17225328/facebook–ads–free–paid–service–mark–zuckerberg.

15 *Id.*

16 *Id.*

17 *See* Paul Hitlin & Lee Rainie, *Facebook Algorithms and Personal Data*, PEW RESEARCH CENTER (Jan. 16, 2019), https://www.pewresearch.org/internet/2019/01/16/facebook–algorithms–and–personal–data/.

18 *Id.*

19 *Id.* at 2.

their interests, roughly half of Facebook users (51%) say they are not comfortable that the company created such a list.[20] The survey also asked targeted questions about two of the specific listings that are part of Facebook's classification system: users' political leanings, and their racial and ethnic "affinities."[21]

As of 2019, 788.4 million people across the globe use Instagram's platform at least once per month.[22] Annual Instagram advertising revenues were $13.86 billion in 2020.[23] In 2012, Facebook acquired Instagram for $1 billion.[24] Since the acquisition, ads across both platforms must be created through Facebook's Ad Manager, even if the business only wants to run their ad on one platform and not the other.[25] This allows advertisers to access specific data regarding ad interactions on Facebook, and also allows Facebook to utilize the information it's able to gather across both accounts so that ads can be targeted to you across both apps.[26] This is echoed in Instagram's privacy policy.[27] "When you visit [Instagram], we may use cookies and similar technologies like pixels, web beacons, and local storage to collect information about how you use Instagram and provide features to you," the policy states.[28] "We may ask advertisers or other partners to serve ads or services to your devices, which may use cookies or similar technologies placed by us or a third party."[29]

As of 2020, Twitter has over 300 million monthly active users.[30] In 2020, Twitter reported total annual revenue of $3.7 billion, a significant increase from the past year[31] Advertising makes up 86% of Twitter's revenue in 2020.[32] Over half of global Twitter revenue is generated in the

---

20 *Id.* at 1.

21 *Id.* at 2.

22 Jasmine Enberg, *Global Instagram Users 2019 Strong Growth Keeps Competition at Bay and Compensates for Facebook's Struggles*, EMARKETER (Dec. 12, 2019), https://www.emarketer.com/content/global–instagram–users–2019.

23 Guttmann, *Annual Instagram advertising revenues in the U.S. from 2018–2023*, STATISTA (Nov. 16, 2020), https://www.statista.com/statistics/1104447/instagram–ad–revenues–usa/.

24 Sam Shead, *Facebook owns the four most downloaded apps of the decade*, BBC NEWS (Dec 18, 2019), https://www.bbc.com/news/technology–50838013.

25 Alli Hoff Kosik, *Here's What You Should Know If You're Worried About Instagram Collecting Your Data*, BUSTLE (Mar. 28, 2018), https://www.bustle.com/p/is–instagram–collecting–data–heres–what–to–know–if–youre–worried–about–your–privacy–8631780.

26 *Id.*

27 *Id.*

28 *Id.*

29 *Id.*

30 Mansoor Iqbal, *Twitter Revenue and Usage Statistics (2022)*, BUSINESS OF APPS (Jan. 11, 2022), https://www.businessofapps.com/data/twitter–statistics/.

31 *Id.* at 3.

32 *Id.*

U.S.[33] In 2020, U.S. Twitter revenue came in at $2 billion, while international revenue was worth $1.6 billion.[34] Twitter generates most of its advertising revenue by selling promoted products, including promoted tweets, promoted accounts, and promoted trends, to advertisers.[35] The company creates specific and individualized advertising opportunities by using an algorithm to make sure promoted products make it into the right users' feeds, timelines, "Who to Follow" lists, or at the top of the list of trending topics for an entire day in a particular country or globally.[36] Advertisers also have the option of paying for video ads delivered to a targeted audience before a video plays, or sponsoring video content from publishing partners.[37] While the majority of revenue from advertising services is generated through Twitter's owned and operated platform, a small portion of the advertising products Twitter sells are also placed on third–party publishers' websites, applications and other offerings.[38]

III. CONSUMER PROTECTION VICTORIES AND LOSSES

Federally legislated data privacy laws would supersede any state data usage laws and would provide a foundation for states to build upon.[39] In 2017, the Equifax data breach infuriated consumers and put their personal and financial information at risk.[40] This scandal brought consumer privacy legislation to the forefront of Congressional business. However, recent attempts to pass a consumer protection bill through Congress have been overlooked. In addition to federal laws and regulations, the U.S. has hundreds of data privacy and data security laws among its states, territories, and localities.[41] Currently, twenty–five U.S. state attorneys general oversee data privacy laws governing the collection, storage, safeguarding, disposal, monitoring, and use of personal data collected

---

33 *Id.* at 3.

34 *Id.*

35 Nathan Reiff, *How Twitter Makes Money*, INVESTOPEDIA (Nov. 6, 2020), https://www.investopedia.com/ask/answers/120114/how–does–twitter–twtr–make–money.asp.

36 *Id.*

37 *Id.*

38 *Id.*

39 *See* Lesley Daunt, *State vs. Federal Law: Who Really Holds the Trump Card?*, THE HUFFINGTON POST (Jan. 28, 2014), https://www.huffpost.com/entry/state–vs–federal–law–who–_b_4676579.

40 *See* Victora Cavaliere & Brian Fung, *Equifax exposed 150 million Americans' personal data. Now it will pay up to $700 million*, CNN (July 22, 2019), https://www.cnn.com/2019/07/22/tech/equifax–hack–ftc/index.html.

41 Angelique Carson, *Data privacy laws: What you need to know in 2020*, OSANO (June 24, 2020), https://www.osano.com/articles/data–privacy–laws.

from their residents, especially regarding instances of data breaches regarding the security of Social Security numbers.[42] Some apply only to governmental entities, some apply only to private entities, and some apply to both. Congress has thus far failed to pass comprehensive data privacy legislation. However, California has led the way in passing the strongest consumer protection bills in the nation.[43]

A. The Equifax Breach

The 2017 Equifax breach eviscerated public trust in corporations and their data protection practices. Over 143 million Americans had their names, addresses, dates of birth, Social Security numbers, and drivers' license numbers exposed to hackers who had access to Equifax's system for months.[44] Over 200,000 users had their credit card information stolen as well.[45] Even after Equifax reinvested in its data security and compensated consumers for having their data stolen, the company continues to collect, bundle, and sell data to large financial institutions.[46]

In 2019, the Federal Trade Commission (FTC) fined Equifax up to $700 million for failing to properly secure its network.[47] The FTC delegated $300 million of the amount to a fund that provided credit monitoring services and compensated anyone who bought such products from Equifax as a result of the data breach.[48] The FTC instructed an extra $125 million to go into a fund, should that $300 million not suffice.[49] Forty–eight states, the District of Columbia and Puerto Rico split another $175 million in civil penalties, and the Consumer Financial Protection Bureau (CFPB) received the final $100 million.[50]

---

42 *Id.*

43 *Id.*

44 Josh Fruhlinger, *Equifax data breach FAQ: What happened, who was affected, what was the impact?*, CYBER SECURITY ONLINE (Feb. 12, 2020, 5:09 AM PST), https://www.csoonline.com/article/3444488/equifax–data–breach–faq–what–happened–who–was–affected–what–was–the–impact.html.

45 *Id.*

46 Katie Lobosco, *Why Equifax will continue to profit by selling your personal information*, CNN MONEY (Oct. 4, 2017, 1:12 PM EST), https://money.cnn.com/2017/10/03/pf/equifax–profit/index.html.

47 Thomas Brewster, *Equifax Just Got Fined Up To $700 Million For That Massive 2017 Hack*, FORBES (Jul. 22, 2019, 10:01 AM EDT), https://www.forbes.com/sites/thomasbrewster/2019/07/22/equifax–just–got–fined–up–to–700–million–for–that–massive–2017–hack/?sh=7e526713e96d.

48 *Id.*

49 *Id.*

50 *Id.*

B. Past Congressional Failure

As Big Tech and social media companies rapidly gain influence and power, state and local leaders have turned to Congress to pass a federal data protection act. Federal leadership on this matter would move the process from a diverse and often complicated array of state and local solutions to the federal level, where the government would respond to privacy infringement issues in a uniform manner. A national data protection act, or DPA, would promote privacy and safety for users, but also for the companies who collect and analyze data while additionally implementing crucial compliance controls. Creating a national strategy while keeping every interest group in mind will allow companies to better understand their responsibilities and related enforcement, and therefore will be able to more effectively and efficiently protect their customers' data. Moreover, the FTC has repeatedly failed to enforce its own orders and has missed opportunities to act on dozens of detailed consumer privacy complaints alleging unfair practices concerning data collection, marketing to minors, cross–device tracking, consumer profiling, user tracking, discriminatory business practices, and data disclosure to third–parties.[51]

The United States does not currently have one federal data privacy law. There is a complex and piece–meal approach for sector–specific and medium–specific laws, including laws and regulations that address telecommunications, health information, credit information, financial institutions, and marketing.[52] The FTC has broad jurisdiction over commercial organizations under its authority to prevent unfair or deceptive trade practices.[53] While the FTC does not explicitly lay out what information should be included in website privacy policies, it has the authority to issue regulations, enforce privacy laws, and take enforcement actions to protect consumers.[54]

In 2018, the Cambridge Analytica scandal came to light as the political analysis firm harvested data from over 87 million Facebook users.[55] The company exploited Facebook's data selling practices, as it continued to

---

[51] *Confronting A Data Privacy Crisis, Gillibrand Announces Landmark Legislation To Create A Data Protection Agency*, KIRSTEN GILLIBRAND: UNITED STATES SENATOR FOR NEW YORK (Feb. 13, 2020), https://www.gillibrand.senate.gov/news/press/release/confronting–a–data–privacy–crisis–gillibrand–announces–landmark–legislation–to–create–a–data–protection–agency.

[52] Carson, *supra* note 41.

[53] *Id.*

[54] *Id.*

[55] *See* Alix Langone, *Facebook's Cambridge Analytica Controversy Could Be Big Trouble for the Social Network. Here's What to Know*, TIME (Apr. 4, 2018, 5:15 PM EST), https://time.com/5205314/facebook–cambridge–analytica–breach/.

buy information from a researcher who told Facebook the data was strictly for academic purposes.[56] The massive abuse of data infuriated the company's investors and caused Facebook's market cap to drop $50 billion in two days.[57] While under investigation by the FTC, Facebook announced nine ways that the company planned to restrict data access.[58] However, Congress failed to fundamentally change the way Big Tech collects and distributes user data, and the FTC simply fined Facebook for its egregious privacy failure.[59]

Over the past few years, members of both parties have introduced data privacy legislation, but Congress has not implemented a new significant federal law on the matter. In December 2019, Senate Democrats unveiled their data privacy bill which begins to establish federal standards resembling California's CCPA (California Consumer Privacy Act), but lacked sufficient bipartisan support.[60] Democrats hoped to strengthen the FTC's authority in regulating Big Tech giants, especially after the Commission's settlements with both Facebook and YouTube.[61] In March 2020, Republicans introduced the Consumer Data Privacy and Security Act of 2020 (CDPSA) which sought to expand protections for small businesses when faced with privacy issues.[62] More significantly, however, the proposed law eliminated the right for private action against companies who commit privacy violations.[63]

Both parties have failed to compromise and agree on terms for a comprehensive data privacy law. Failure to implement significant policy would allow data breaches and mismanagement to continue plaguing Big Tech. The Equifax breach and the Cambridge Analytica scandal have exemplified that FTC fines do not significantly impact the practices of these corporations. Legislative action with genuine repercussions would

---

56 *Id.*

57 *Id.*

58 Mike Schroepfer, *An Update on Our Plans to Restrict Data Access on Facebook*, META (Apr. 4, 2018), https://about.fb.com/news/2018/04/restricting–data–access/.

59 *See* Mike Snider & Edward C. Baig, *Facebook fined $5 billion by FTC, must update and adopt new privacy, security measures*, USA TODAY (Jul. 24, 2019, 7:14 PM EST), https://www.usatoday.com/story/tech/news/2019/07/24/facebook–pay–record–5–billion–fine–u–s–privacy–violations/1812499001/.

60 Lauren Feiner, *Senate Democrats reveal new digital privacy bill that would strengthen the FTC's enforcement powers over tech companies*, CNBC (Nov. 26. 2019, 9:57 AM EST), https://www.cnbc.com/2019/11/26/senate–democrats–reveal–new–copra–digital–privacy–bill.html.

61 *Id.*

62 Gregory Katofil, *Federal Privacy Legislation Update: Consumer Data Privacy and Security Act of 2020*, THE NAT'L L. REV., VOLUME X, NO. 74 (Mar. 14, 2020), https://www.natlawreview.com/article/federal–privacy–legislation–update–consumer–data–privacy–and–security–act–2020.

63 *Id.*

likely have a greater impact on the data collection practices of these companies, and California has begun to lead this effort in recent years.

B. The California Blueprint

California's reputation for trailblazing progressive policies continued in 2019 with the passage of the California Consumer Privacy Act (CCPA), which, at the time, was the strongest consumer and data privacy protection law in the nation.[64] The passage of the CCPA allows Californians "the right to: know what personal information of theirs is being collected; know whether the information is being sold or disclosed and to whom; and finally, say no to the sale of personal information."[65] Mirosofts quickly announced that it would adhere to the CCPA by applying such consumer protection standards nationally.[66] Facebook, however, has chosen to fight the CCPA by exploiting a potential loophole.[67] By giving third party businesses its web tracker, Pixel, Facebook argues that because the companies, not Facebook, are collecting the users' data, Facebook cannot be held liable for fines under the CCPA.[68]

In November 2020, California voters approved Proposition 24, or the California Privacy Rights Act (CPRA), which further expands the CCPA.[69] The Proposition allows consumers to: prevent businesses from sharing personal information; correct inaccurate personal information; and lastly, limit businesses' use of "sensitive personal information."[70] Such information includes precise geolocation; race; ethnicity; religion; genetic data; union membership; private communications; and certain sexual orientation, health, and biometric information.[71] The CPRA establishes a California Privacy Protection Agency (CalPPA) to enforce and implement consumer privacy laws, and impose administrative fines and prohibit

---

64 *See* Sara Morrison, *California's new privacy law, explained*, VOX (Dec. 30, 2019, 6:50 PM EST), https://www.vox.com/recode/2019/12/30/21030754/ccpa–2020–california–privacy–law–rights–explained.

65 *Id.*

66 *See* Julie Brill, *Microsoft will honor California's new privacy rights throughout the United States*, MICROSOFT (Nov. 11, 2019), https://blogs.microsoft.com/on–the–issues/2019/11/11/microsoft–california–privacy–rights/.

67 *See* Sara Morrison, *Facebook is gearing up for a battle with California's new data privacy law*, VOX (Dec. 17, 2019, 5:00 PM EST), https://www.vox.com/recode/2019/12/17/21024366/facebook–ccpa–pixel–web–tracker.

68 *Id.*

69 *See* Sara Morrison, *California just strengthened its digital privacy protections even more*, VOX (Nov. 4, 2020, 12:06 PM EST), https://www.vox.com/2020/11/4/21534746/california–proposition–24–digital–privacy–results.

70 *Id.*

71 *Id.*

businesses' retention of personal information for longer than reasonably necessary.[72]

According to Jones Day, the CPRA expands the private right of action to apply to data breaches.[73] Previously, consumers did not have many viable options to litigate these claims and solely relied on state or federal bodies to enforce the consumers' data protection rights.[74] Similarly, businesses providing services to minors may have heightened risk for fines equaling triple the maximum penalty for each violation.[75] The CPRA limits the defense that businesses may have to private actions, providing that "the implementation and maintenance of reasonable security procedures and practices . . . following a breach does not constitute a cure with respect to that breach."[76] In March 2020, Washington State failed to pass a law similar to CPRA solely because the legislature could not agree on whether individuals should have the right to take direct legal action.[77] As arguably the most contentious aspect of the CPRA, legislatures across the nation must decide how to address this part of the law.

Only a few of the CPRA's provisions go into effect immediately, with most of its provisions not becoming operative until January 1, 2023.[78] The new law finds precedent in the implementation of the European Union's General Data Protection Regulation (GDPR).[79] The GDPR entered into force on May 24, 2016, but did not become effective until May 25, 2018.[80] In theory, the delayed implementation provided companies with two years to establish feasible ways to ensure compliance with the updated law.[81] The GDPR governs the collection, use, transmission, and security of data collected from residents of any of the twenty–eight member countries of the European Union. The law applies to all EU residents, regardless of the

---

72 *Id.*

73 Jones Day, *California Voters Adopt the California Privacy Rights Act*, JONES DAY (Nov. 2020), https://www.jonesday.com/en/insights/2020/11/california–voters–approve–cpra.

74 *Id.*

75 *Id.*

76 *Id.*

77 *See* Khari Johnson, *Washington Privacy Act fails again, but state legislature passes facial recognition regulation*, VENTURE BEAT (Mar. 12, 2020), https://venturebeat.com/2020/03/12/washington–privacy–act–fails–in–state–legislature–again/.

78 Jones Day, *supra* note 73.

79 *See* David Strauss, *CCPA 2.0: Analysis of the California Privacy Rights Act's Implementation Timeline*, HUSCH BLACKWELL (May 11, 2020), https://www.bytebacklaw.com/2020/05/ccpa–2–0–analysis–of–the–california–privacy–rights–acts–implementation–timeline/.

80 *Id.*

81 *Id.*

entity's location that collects the personal data.[82] Fines of up to €20 million or 4% of total global turnover may be imposed on organizations that fail to comply with the GDPR.[83]

Under the GDPR, consumers have greater control over what they consent to while navigating through websites.[84] The consent must be easy to withdraw, and for someone under sixteen, a person holding "parental responsibility" must opt in to data collection on their behalf.[85] Moreover, under the new regulations, companies must notify their data protection authority about a data breach within seventy–two hours of first becoming aware of it.[86]

IV. REINFORCING CONSUMER PROTECTIONS

The federal government has allowed Big Tech and social media companies to profit off data provided by their users for nearly two decades. Users' hands are forced in agreeing to the terms and conditions of these companies, as the influence of these companies has become too much to resist. Congress must implement a bipartisan solution to the unethical collection of data and infringement of privacy by either creating a data tax, or by passing a comprehensive data protection act to curb these limitless data collection practices. Additionally, should a consumer's rights be violated, the consumer should have the right to take legal action against the entity rather than hope that state prosecutors pursue the case. California's CPRA addresses these issues and provides a legitimate solution to the nation's data privacy problem. Alternatively, Apple has recently begun self–regulating data collection policies on all apps which it supports through its iOS, which may lead to heightened consumer protection.[87] As one of the most influential tech companies in the world, Apple's new regulations may force companies to tighten their data privacy practices. This would prioritize the needs of consumers over corporate profits.

---

82 *Id.*

83 *Id.*

84 *See* Arjun Kharpal, *Everything you need to know about a new EU data law that could shake up big US tech*, CNBC (May 25, 2018, 12:29 PM EST), https://www.cnbc.com/2018/03/30/gdpr–everything–you–need–to–know.html.

85 *Id.*

86 *Id.*

87 *See* Bernard Marr, *Apple Vs. Facebook – Who Will Win The Data Privacy War?*, FORBES (Feb. 19, 2021, 12:34 AM EST), https://www.forbes.com/sites/bernardmarr/2021/02/19/apple–vs–facebook—who–will–win–the–data–privacy–war/?sh=7fb2bb4b5e14.

A. The Data Tax

Advocates for consumer protection have proposed a minor data tax, between .8 and 1 percent, which would be implemented across the entire industry of selling users' personal information. With social media companies generating billions of dollars every year, a fractional data tax will not considerably impact the bottom line. Saadia Madsbjerg argues that the data tax would be nothing more than a sales tax, as users' data has become increasingly valuable and is the commodity being sold.[88] Although access to "free" platforms on the internet must come at a cost, the imbalance of power has paved the way for this necessary change. When considering options quickly, a broad data tax presents an appealing option for governments to give consumers just compensation for data. The tax would be relatively simple to implement, despite the potential difficulty in measuring the true value added in Big Tech's digital economy and business model. Most importantly, a data tax would not require a direct measure of how valuable each piece of personal data and information is worth.[89] Such an undertaking would prove tedious and time consuming, and would likely clog up the tax's overall implementation and success. According to the Los Angeles Times, the data brokerage industry generated $200 billion in 2019; a data tax of even 1 percent would generate over $2 billion.[90]

Even if corporations and small businesses alike choose to continue harvesting consumers' data, a tax would begin to rebalance the power struggle that corporations have imposed on users. Axios reported that on average, Facebook values each of its users at $7.37 and Twitter $2.83.[91] Big Tech giants should pay their fair share in profiting off of information shared by its users. In 2019, California Governor Gavin Newsom announced his interest in implementing a "data dividend," which would allow consumers to reap the benefits of providing their information to corporations.[92] Newsom justifies this stance by emphasizing that Big Tech

---

88 *See* Saadia Madsbjerg, *It's Time to Tax Companies for Using Our Personal Data*, THE NEW YORK TIMES (Nov. 14, 2017), https://www.nytimes.com/2017/11/14/business/dealbook/ . . . .taxing–companies–for–using–our–personal–data.html.

89 *Id.*

90 *Id.*

91 *See* Sara Fischer, *Reddit's exponential valuation rise*, AXIOS (Feb. 12, 2019), https://www.axios.com/reddits–exponential–valuation–17295eb2–28e5–47bf–a2db–caa5d488e3af.html.

92 Jeff Daniels, *California governor proposes 'new data dividend' that could call on Facebook and Google to pay users*, CNBC (Feb. 12, 2019, 9:36 AM EST), https://www.cnbc.com/2019/02/12/california–gov–newsom–calls–for–new–data–dividend–for–consumers.html.

giants make billions of dollars collecting, curating and monetizing our personal data, so they should have an equally important duty to protect it.[93]

In 2020, a global tax watchdog, the Organization for Economic Cooperation and Development (OECD) proposed an overhaul of international tax rules to make sure big tech companies pay their dues, and warned that failure to adopt it would make the economic recovery from COVID–19 harder.[94] The group has tried to balance the demands of over 135 countries, but the U.S. has long resisted the type of regulation being discussed.[95] Cross–border taxation has become tricky as companies have sold digital services, rather than physical goods.[96] They can easily move their headquarters to low–tax countries, recording profits and parking assets like trademarks and patents in those jurisdictions to avoid paying the governments of the places where they do business, or were founded.[97] In early 2021, the OECD negotiations resumed and most participants indicated that they prefer an international agreement rather than unilateral measures.[98] Amazon, Google, and Facebook all released statements supporting OECD's efforts to create a strongly supported system.[99]

B. Implementing a Federal Data Privacy Standard

In creating a federal baseline for consumer protection and privacy rights, the federal government must create a floor, not a ceiling. Although the federal government would establish the standards that companies and data collection groups would adhere to, individual states will continue to be responsible for administering and policing the new law. Some states, such as California, will likely go above and beyond the requirements of the federal law and allow, for example, individuals to litigate their claims against companies themselves. Congress would work with Big Tech companies, consumer rights groups, and data privacy activists in order to hear all sides of the issue. However, as Congress' previous attempts have shown, balancing the interests of all parties affected has proven to be quite a feat.

---

93 *Id.*

94 *See* Kelvin Chan, *Global watchdog proposes tax overhaul*, ASSOCIATED PRESS (Oct. 12, 2020), https://apnews.com/article/technology–business–paris–france–tax–reform–bc18de1f6f3e657f6162b4c2e810f21b.

95 *Id.*

96 *See* Evie Liu, *The OECD Wants Big Tech to Pay More Taxes*, BARRON'S (Oct. 9, 2019, 3:18 PM EST), https://www.barrons.com/articles/oecd–tax–reform–big–tech–google–digital–economy–51570648654.

97 *Id.*

98 David McHugh, *Debate heats up over how countries tax Big Tech companies*, ABC NEWS (Jan. 27, 2021, 8:07 AM EST), https://abcnews.go.com/Business/wireStory/debate–heats–countries–tax–big–tech–companies–75510363.

99 *Id.*

Mark Zuckerberg met with a group of senators in September 2019 to discuss Big Tech regulation and potential policy implementation.[100] Facebook had recently settled with the FTC to end its probe into the company's data privacy practices.[101] Zuckerberg expressed that he understood that Big Tech's self–regulation will not work, and that some form of government intervention is necessary.[102] This meeting proved to be a very important first step in bringing the relevant parties to the table in order to implement relevant change. Although Facebook has responded contentiously to California's CCPA and CPRA, the state law has given federal lawmakers ideas as to how a national strategy could be implemented.[103]

Almost every federal privacy bill in recent Congressional sessions have met the general baseline established by the original CCPA, predominantly through the inclusion of individual privacy rights.[104] Most notably, two recent bills from Senate Commerce Chairman Roger Wicker (R–MS) and Ranking Member Maria Cantwell (D–WA) go further than the CCPA by establishing limits for data collection, use, and sharing while also applying those obligations to third parties that receive personal information.[105] Cantwell's bill, the Consumer Online Privacy Rights Act (COPRA) and Wicker's bill, the SAFE DATA Act, address many of the same issues, but approach the concepts differently.[106]

Both bills adopt the same general framework: a set of individual rights combined with boundaries on how businesses collect, use, and share information, all of which would be enforced through the FTC.[107] The individual rights include access, correction, deletion, and portability for personal information, along with rights to give "affirmative express consent" before the collection and processing of "sensitive" categories of information and to opt out of the sale or transfer of personal data.[108] Business obligations include data minimization, use limitations, data

---

100 Feiner, *supra* note 60.

101 *Id.*

102 *Id.*

103 *See* Jon Swartz, *California's landmark privacy law is Facebook's next 'nightmare'*, MARKETWATCH (Aug. 22, 2020, 10:36 AM EST), https://www.marketwatch.com/story/californias–landmark–privacy–law–is–facebooks–next–nightmare–2020–08–18.

104 Cameron F. Kerry & Caitlin Chin, *By passing Proposition 24, California voters up the ante on federal privacy law*, BROOKINGS (Nov. 17, 2020), https://www.brookings.edu/blog/techtank/2020/11/17/by–passing–proposition–24–california–voters–up–the–ante–on–federal–privacy–law/.

105 *Id.*

106 *See* Cameron F. Kerry, *Game on: What to make of Senate privacy bills and hearing*, BROOKINGS (Dec. 3, 2019), https://www.brookings.edu/blog/techtank/2019/12/03/game–on–what–to–make–of–senate–privacy–bills–and–hearing/

107 *Id.*

108 *Id.*

security, and the responsibility to bind other companies that receive personal information to the same obligations.[109] In addition, both bills expand FTC enforcement authority, with state attorney general enforcement authority as force multipliers, and give the agency power to interpret specific provisions by adopting rules and expanded legal authority.[110]

However, the recent passage of the CPRA changes the thinking behind a federal standard, as the California law has incorporated many of these same provisions.[111] Nevertheless, there are still several areas where federal legislation can offer greater protections, such as the private right of action, establishing small business requirements, and protecting consumers against algorithmic discrimination.[112] Similarly, a federal standard for consumer privacy rights would be applauded by consumers in states with no such protections. Recent settlements over the past ten years with the FTC have demonstrated that federal fines for privacy–violating corporations are often simply viewed as the cost of doing business, not a call to change these vicious practices.[113] To make privacy protections meaningful, consumers should have the right to sue such violating companies for damages, and the FTC should have the authority to levy civil penalties and to set strong privacy rules.[114]

i. Private Right of Action:

Politicians on both sides of the aisle have debated whether individuals should be able to bring legal actions under privacy laws.[115] Earlier this year, a Washington State privacy bill failed to pass due to this very issue.[116] In order to ease the fears of business leaders in California, referendum leader Alastair Mactaggart proposed a limited private right of action in both the CCPA and CPRA.[117] As seen in both Washington and California, balancing the interests of all parties considered paves the way for successful legislation. The CCPA narrowly allows individuals to sue for cases of "unauthorized access and exfiltration, theft, or disclosure of a consumer's nonencrypted or nonredacted personal information," and

---

109 *Id.*
110 *Id.*
111 *See generally* Jones Day, *supra* note 73.
112 *See* Kerry & Chin, *supra* note 104.
113 *See* Neema Singh Guliani & Kate Ruane, *Senators Reveal Their Plans to Protect Consumer Privacy Online*, AMERICAN CIVIL LIBERTIES UNION (Dec. 5, 2019), https://www.aclu.org/news/privacy–technology/senators–reveal–their–plans–to–protect–consumer–privacy–online/.
114 *Id.*
115 Kerry & Chin, *supra* note 104.
116 Guliani & Ruane, *supra* note 113.
117 Guliani & Ruane, *supra* note 113.

requires potential plaintiffs to give businesses a thirty–day notice and an opportunity to "cure" the issue.[118] The CPRA does not significantly expand this provision, and only clarifies that the disclosure of an email address, combined with a security question or password that would expose access to an online account, constitutes a covered data breach and that businesses cannot "cure" a claim simply by implementing new security procedures following an incident.[119] By narrowing the scope of potential litigation, California lawmakers have given consumers some private recourse in protecting their data while also defending the corporations' course of business.

Consumers have also tested whether the CPRA's right to private action can be applied retroactively. Current California precedent establishes that for a law to be applied retroactively, the law must include an expressly stated retroactivity provision.[120] The CPRA does not currently include such a provision, but lawsuits have already attempted to apply the law retroactively.[121] Congress should take Mactaggart's leadership as a starting point, but consumer rights activists have stressed the importance of a more expansive right of private action against corporations.

ii. Small Businesses Requirements:

From local to federal, most legislation comes with its fair share of loopholes, and the CCPA is no exception. The California law has a significant and sweeping exemption: it does not apply to any organization that annually generates under $25 million, earns less than 50% of revenue from selling consumer data, and processes data from less than 50,000 entities.[122] Even though the CPRA alters the standards of this exemption, it does not completely remove them.[123] By permitting exceptions for small businesses, consumers continue to worry about the safety of their personal information. Although small businesses provide crucial services and provide jobs for millions of Americans, consumer rights advocates have begrudgingly accepted this exception.

---

118 Guliani & Ruane, *supra* note 113.

119 Guliani & Ruane, *supra* note 113.

120 Evangelatos v. Superior Court, 753 P.2d 585, 639 (Cal. 1988).

121 Cathy Cosgrove, *The private right of action*, THE INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (June 8, 2020), https://iapp.org/news/a/ccpa–litigation–shaping–the–contours–of–the–private–right–of–action/.

122 *See* Anna Attkisson, *How California's Consumer Privacy Act Will Affect Your Business*, BUSINESS NEWS DAILY (Dec. 31, 2019), https://www.businessnewsdaily.com/10960–ccpa–small–business–impact.html.

123 Elizabeth Harding, *CPRA – What This Means For Your Business*, THE NAT'L L. REV. (Nov. 9, 2020), https://www.natlawreview.com/article/cpra–what–means–your–business

Closing the small business loophole when applying a federal data privacy law would likely provide stronger protections for consumers and their data. Cantwell and Wicker's legislation take separate approaches: COPRA broadly exempts businesses that do not meet certain size or revenue requirements from all provisions of the bill, while the SAFE DATA Act only exempts them from certain ones.[124] In order to satisfy both sides, businesses should face liability depending on how the size and complexity of the covered entity, scope of covered data, and possible privacy risks, with some additional requirements or exemptions for large or small data holders.[125] Creating these general standards of responsibility would establish some sort of baseline to protect privacy for all organizations, while avoiding an unmanageable burden for smaller businesses.[126]

iii. Algorithmic discrimination

The CCPA does not directly address algorithmic discrimination, although the CPRA does give individuals the right to turn off automated decision–making while accessing a company's website.[127] Algorithms and machine learning have the potential to use personal information and consumer preferences in ways that could benefit individuals, such as alert them to new product offerings of services. However, this technology has the propensity to harm individuals as well. This becomes a civil rights issue if algorithms make decisions that could limit options or opportunities for marginalized groups of people or otherwise violate existing federal or state anti–discrimination laws.[128]

The Wicker and Cantwell bills both go beyond the algorithmic discrimination standards established by the CCPA and CPRA. However, significant differences between the approaches exist. Wicker's bill allows the FTC to refer information about instances of likely anti–discrimination laws to relevant government agencies and also recommends the FTC issue algorithmic transparency reports.[129] However, the FTC already has the authority to refer such information in multiple contexts, so this proposed solution likely will not achieve its intended goal.[130] Meanwhile, Cantwell's bill requires businesses to conduct annual "algorithmic decision–making impact assessments" and holds that any violation of

---

124 Kerry & Chin, *supra* note 104.
125 Kerry & Chin, *supra* note 104.
126 Kerry & Chin, *supra* note 104.
127 Kerry & Chin, *supra* note 104.
128 Kerry & Chin, *supra* note 104.
129 Kerry & Chin, *supra* note 104.
130 Guliani & Ruane, *supra* note 113.

anti–discrimination laws is also a violation of the FTC Act.[131] This significant change would directly impact the way the federal government regulates companies. Additionally, Cantwell's bill includes provisions that would prohibit the use of data to discriminate in housing, employment, credit, education, or public accommodations, and permits the FTC to enforce the prohibition.[132]

Under any sort of federal privacy law passed in Congress, companies should observe a "duty of care" against processing or transferring covered data in a manner that could violate existing anti–discrimination laws, in addition to the legislative provisions from Wicker and Cantwell.[133] As consumer privacy becomes more prevalent, a federal privacy law could go well beyond the CPRA. Congress has a duty to end discrimination in all forms and could continue its work in doing so by holding businesses responsible and accountable. This includes when a corporation creates and implements algorithms which have an inherently prejudicial impact on higher risk or marginalized populations.

C. The Potential of Self–Regulation

In January 2021 at a data privacy conference in Brussels, Apple CEO Tim Cook announced Apple's new App Tracking Transparency regulation software.[134] In his presentation, Cook focused on the problematic practice tech companies utilize to generate revenue: intentionally misleading users.[135] Although Cook did not mention Facebook by name, he did hint to platforms which decrease public trust in vaccines and serve targeted ads which often led to real world violence.[136] Based on user preferences and data, Facebook previously recommended extremist groups to users through its algorithms, but the company recently announced it would end such recommendations.[137] After the conference, Zuckerberg slammed Cook and claimed that Apple's privacy changes come as a way for the company to disadvantage Facebook.[138]

With App Tracking Transparency, Apple will require every iOS app to ask users upfront if Apple has permission to share their information with

---

131 Kerry & Chin, *supra* note 104.
132 Guliani & Ruane, *supra* note 113.
133 Kerry & Chin, *supra* note 104.
134 *See* Kif Leswing, *Apple CEO links Facebook's business model to real–world violence*, CNBC (Jan. 28, 2021), https://www.cnbc.com/2021/01/28/apple–ceo–tim–cook–says–f.html.
135 *Id.*
136 *Id.*
137 *Id.*
138 *Id.*

data brokers and other networks.[139] If users give their permission, the app can then serve mobile ads to them and measure their response to those ads.[140] After this change is in place, users will see a notification the first time they launch any new app on their phone, explaining what the proposed third–party tracker is used for, and whether the user wants to approve or reject the tracking and sharing of their data.[141] When these changes become implemented in spring 2021, Apple will begin its role as self–regulator of data privacy rights.[142]

On the other hand, Facebook's recent data privacy changes have infuriated its users.[143] Currently, WhatsApp allows users to communicate with businesses through WhatsApp chat, and some of those businesses are hosted by Facebook.[144] According to the new policy, messages between the user and the business they communicate with could be collected and shared with the larger Facebook ecosystem.[145] Essentially, Facebook and its advertisers would now be able to use customer service chats or transaction receipts for marketing and advertising purposes.[146]

The content of users' individual chats will continue to be encrypted, so they cannot be seen by the company, and data within those chats will not be harvested or shared with third parties.[147] Nonetheless, Facebook faced backlash against the new rules after the announcement, prompting them to publish an FAQ page to clarify the policy and reassure upset WhatsApp users.[148] This stark policy difference highlights the path two Big Tech giants have chosen to take in the midst of potential government regulation and data–taxing. Apple has attempted to provide transparency while bringing the needs of its users to the forefront, while Facebook continues to prioritize its advertisers over its users.[149]

Microsoft, on the other hand, has learned its lesson about waiting for government regulation after its 2001 settlement with the FTC.[150] The government accused Microsoft of illegally maintaining its monopoly

---

139 *Id.*
140 Marr, *supra* note 87.
141 Marr, *supra* note 87.
142 Marr, *supra* note 87.
143 Marr, *supra* note 87.
144 Marr, *supra* note 87.
145 Marr, *supra* note 87.
146 Marr, *supra* note 87.
147 Marr, *supra* note 87.
148 Marr, *supra* note 87.
149 Marr, *supra* note 87.
150 Steve Denning, *Why Big Tech Should Regulate Itself*, FORBES (Aug. 2, 2020, 6:33 PM EDT), https://www.forbes.com/sites/stevedenning/2020/08/02/why–big–tech–should–regulate–itself/?sh=69083f602677.

position in the PC market.[151] Eventually, the company agreed to a settlement which devastated the company's ingenuity and entrepreneurial spirit for more than a decade.[152] Since then, Microsoft has strived to prioritize the needs and rights of its users over earning every last drop of profit from their advertisers.[153] When the EU proposed the GDPR, Microsoft immediately supported the regulation by putting customers in control of their own data.[154]

V. THE RESULTS OF REGULATION

Throughout this nation's history, the government has regulated industries which became too large and powerful in an effort to eliminate monopolies, promote consumerism, and improve society as a whole. Regulating the data collection and sales practices of Big Tech giants would both rein in the corporations' power and control over users' consumer behavior while also protecting the privacy and security of users' personal information. The federal government should provide consumers with these safeguards as an effort to reinforce public trust in the services and companies individuals rely so heavily on.

A. Effects of the Data Tax

The funds generated by the data tax would likely see the greatest results if put towards think tanks and lobbyists who would push for stronger consumer protection bills in Congress. Because these social media companies operate globally, Congressional action is necessary to begin the process of lessening their power and prioritizing consumer welfare over corporate profits. Currently, the digital economy is growing two and a half times faster than global GDP, and governments are trying to tax the resulting revenue.[155] Although some corporations, such as Microsoft, have begun adhering to state laws, a federal law would set the tone for data privacy practices moving forward. Reining in the power of Big Tech would leave consumers and society as a whole better off. The tax collected could, in turn, fund better research on the digital economy, more competitive salaries for public tech experts, and more robust

---

151 *Id.*
152 *Id.*
153 *Id.*
154 Brill, *supra* note 66.
155 Amie Ahanchian, Donald Hok, Philippe Stephanny, Elizabeth S. Shingler, *Digital Services Tax: Why the World is Watching*, BLOOMBERG TAX (Jan. 6, 2021, 3:01 AM), https://news.bloombergtax.com/daily–tax–report/digital–services–tax–why–the–world–is–watching.

oversight of digital business.[156] Eventually, governments could use tax incentives to encourage compliance with whatever new rules on data privacy societies choose to develop.[157]

In 2018, the European Commission (EC) proposed the imposition of a temporary Digital Services Tax (DST) at a rate of 3% on revenues derived from online advertising services, receipts or income from digital intermediary activities, and sales of user–collected data.[158] Businesses with annual worldwide revenues exceeding $915 million (€750 million), and taxable revenues within the EU exceeding $61 million (€50 million) would be subject to the tax.[159] The sourcing of DST revenue is generally based on whether the taxed service is viewed or enjoyed by a user that has a device located in the jurisdiction imposing the DST.[160]

A device is generally deemed located in a DST jurisdiction based on its internet protocol address (IP address) or any geolocation method.[161] Although the EC rejected the measure, various countries across Europe have implemented their own version of a DST.[162] There are, of course, variations among DSTs.[163] For instance, Austria applies its DST only to digital advertising, while Poland assesses its DST only on streaming services.[164] Alternatively, Turkey levies its DST on digital content as well as advertising, intermediary activities, and the sale of user data.[165] India and Kenya, on the other hand, tax receipts from a broad variety of digital services.[166]

B. Effectiveness of a Federal Data Privacy Law

In understanding the potential success of a federal data privacy law, Congress should look to other federal privacy laws, such as the Health Insurance Portability and Accountability Act (HIPAA). Broadly speaking, the patients receive the greatest benefits of HIPAA protections. HIPAA ensures healthcare providers, health plans, healthcare clearinghouses, and business associates of HIPAA–covered entities must implement multiple

---

156 *Id*.
157 *Id.*
158 *Id.*
159 *Id.*
160 *Id.*
161 Elke Asen & Daniel Bunn, *What European OECD Countries Are Doing about Digital Service Taxes*, TAX FOUNDATION (Nov 22, 2021), https://taxfoundation.org/digital-tax-europe-2020/.
162 *Id.*
163 *Id.*
164 *Id.*
165 *Id.*
166 *Id.*

safeguards to protect sensitive personal and health information.[167] HIPAA established rules that require healthcare organizations to control who has access to health data, restricting who can view health information and who that information can be shared with.[168] Moreover, HIPAA helps to ensure that any information disclosed to healthcare providers and health plans, or information that is created by them, transmitted, or stored by them, is subject to strict security controls.[169] Patients are also given control over who their information is released to and who it is shared with.[170]

Like HIPAA, a federal data privacy act would give consumers more say in who gets access to their data. Little to no regulations on Big Tech exist to oversee who has access to consumer data, who can view consumer data, and who consumer data can be shared with and sold to. The government's failure to regulate this industry played a large role in the Equifax breach of 2017 and the Cambridge Analytica Facebook scandal in 2018 as discussed above. A federal law would set a consistent standard for how companies treat consumers' personal information and would inspire greater confidence in how responsible companies behave.[171] It could address the significant risks posed by the aggregation of consumer profiles, which include racial and economic discrimination and a lack of transparency about how information is collected and used.[172]

Europe's GPDR has seen increased enforcement in fining Big Tech companies for their data collecting violations.[173] The EU law will issue larger fines for data protection violations than have ever been seen before: €20 million, or up to 4% of a company's annual worldwide revenue from the preceding financial year, whichever's greater.[174] The fines have hit two companies so far, the first to the local subsidiary of Facebook in Germany, for €51,000, and the second to Google in France over Android, for €50 million.[175] Regulators also have the power to stop companies either temporarily or permanently from collecting and processing data, which is

---

[167] Steve Adler, *Why is HIPAA Important*, HIPAA JOURNAL (Oct. 12, 2017), https://www.hipaajournal.com/why–is–hipaa–important/.

[168] *Id.*

[169] *Id.*

[170] *Id*.

[171] Peter M. Lefkowitz, *Why America Needs a Thoughtful Privacy Law*, THE NEW YORK TIMES (June 25, 2019), https://www.nytimes.com/2019/06/25/opinion/congress–privacy–law.html.

[172] *Id.*

[173] Katie Collins, *As the GDPR turns 2, Big Tech should watch out for big sanctions*, CNET (May 24, 2020, 5:00 AM PT), https://www.cnet.com/news/as–the–gdpr–turns–2–big–tech–should–watch–out–for–big–sanctions/.

[174] *Id.*

[175] *Id.*

a severe consequence for Big Tech.[176] These new policies have the potential to completely disrupt their business models and force them to make major changes to their core products.[177]

A national privacy statute would also advance other U.S. interests. If legislation passed, the United States could harmonize its laws with those of other major economies, easing trade concerns and promoting American technology in Europe and beyond.[178] For years, the United States has warned against other nations stealing its intellectual property and consumer data.[179] Among other things, with a comprehensive data protection law in place which addresses principles, rather than nationalities, there would be less need to resort to corporate bans or divestment strategies regarding individual foreign technology companies.[180] For example, the United States for years has complained about the fact that American tech platforms such as Google, Facebook, YouTube, Twitter, and WhatsApp are prohibited in China.[181] Longstanding arguments against China's arbitrary application of "national security" policies to disadvantage U.S. firms are undercut by the perception that the United States is emulating the Chinese approach in targeting Chinese social media platforms TikTok and WeChat.[182] A federal data protection regime would place the United States on stronger footing to address concerns posed by Chinese companies without opening up Washington to charges of hypocrisy.[183]

VI. CONCLUSION

For years, Big Tech has exercised near–complete freedom in accessing consumer data and utilizing it to generate an amount of revenue never seen before. Although the companies provide access to their platforms for no monetary cost, that should not grant them the right to completely exploit user data. If Congress does not either implement a data tax or pass a

---

176 *Id.*
177 *Id.*
178 *Id.*
179 David H. Laufman, Joseph M. Casino, Michael J. Kasdan, *The Department of Justice's National Security Division Chief Addresses China's Campaign to Steal U.S. Intellectual Property*, THE NAT'L L. REV. VOL. X, NO. 237 (2020), https://www.natlawreview.com/article/department–justice–s–national–security–division–chief–addresses–china–s–campaign–to.
180 Robert D. Williams, *To enhance data security, federal privacy legislation is just a start*, BROOKINGS (Dec. 1, 2020), https://www.brookings.edu/techstream/to–enhance–data–security–federal–privacy–legislation–is–just–a–start/.
181 *Id.*
182 *Id.*
183 *Id.*

comprehensive federal privacy law, consumers will continue to be manipulated for their private information, and more drastically, fall victim to data breaches and identity theft. As seen with both the Equifax and Cambridge Analytica breaches, consumers have long paid the cost for Big Tech's failure to protect the basic interests of their users. The corporations have begun exploring self–regulation, but these changes alone will not likely amount to the type of change this space requires to level the playing field for consumers.

The current negotiations in Congress make it clear that all affected parties have a different view on how Big Tech giants should be regulated, but our elected officials must come together to prioritize societal good and consumer welfare. Congress should look to the examples set by the EU's GDPR, or California's CCPA and CPRA, to serve as a blueprint for a federal privacy law. These trailblazing policies put the needs of users at the forefront in explicitly protecting their privacy interests. The laws give government bodies the heightened authority necessary to rein in the power of Big Tech's data collection.

CEOs and consumer activist groups have come to the table to discuss their priorities, now Congress must act to meet the needs of all parties in an equitable and just manner. Enacting a federal data privacy law would increase consumer confidence in companies and corporations while also allowing consumers to have more control over the information they provide. The implementation of HIPAA in the medical field exemplifies the importance of privacy rights for individuals, but not just when it comes to health. Data privacy impacts all Americans, as the internet has become a vital part of our society. The sooner our government acts to protect our privacy rights and liberties, the stronger we become as a nation.