3

The Data War

Social Media Kills Privacy

Amidst the partisan rancor that has enveloped the United States since the election of President Donald Trump in November of 2016, exacerbated by the COVID-19 pandemic shutdowns which began in March of 2020, Americans have forgotten that they once agreed on the primary ill of social media: its use of Big Data to invade privacy and manipulate users. Concerns about Big Data, privacy, and the power of digital firms in the knowledge economy lie at the center of Shoshana Zuboff's seminal 2019 book *The Age of Surveillance Capitalism*.[1] Privacy and data protection (or the lack thereof) were also the core concerns driving the Facebook/Cambridge Analytica scandal of 2018, in which a political firm associated with prominent Republicans including Steve Bannon – one of President Trump's most prominent advisers – used data obtained by deceit from Facebook to build profiles of voters.[2] And outside of the United States, it is privacy concerns that motivated the most important early regulatory effort in the world directed at Big Tech, the European Union's General Data Protection Regulation (GDPR), which came into effect in May of 2018.[3] Furthermore, in 2018 the State of California adopted a similar, albeit more limited, data privacy law, the California Consumer Privacy Act (CCPA), which voters amended in 2020 to expand its protections (the new provisions came into effect in 2023).[4] Both the GDPR and CCPA are described in more detail in Chapter 7.

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

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

[3] General Data Protection Regulation 2016/679, 2016 O.J. (L 119), https://gdpr-info.eu/.

[4] Cal. Civ. Code §§ 1798.100–178.99-100. For a good, short summary of the CCPA, *see California Consumer Privacy Act (CCPA)*, Office of the Attorney General, State of California Department of Justice, https://oag.ca.gov/privacy/ccpa#.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 09 Nov 2026 at 06:00:40, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009547703.004

One notable fact about privacy and related concerns raised by Big Data is that they come from across the political spectrum. When the Cambridge Analytica scandal broke, it triggered calls for investigations from both Republican and Democratic leaders in the United States Congress, and generated an investigation by the Democratic attorney general of the State of Massachusetts, Maura Healey (who was later elected governor of that state). Similarly, the GDPR appears to enjoy broad support within the European Union, as does the CCPA in California (except, of course, among tech firms). Moreover, the bipartisan nature of privacy concerns makes sense. The desire to keep one's personal life to oneself surely has no political valence, nor does the desire not to be manipulated (though perhaps there are generational differences regarding both desires). And yet, despite all of the criticisms and scandals, the sound and the fury, the United States Congress has failed to pass any meaningful privacy legislation, and the laws that have passed (notably the GDPR and CCPA) are widely criticized as toothless. Why is this so?

3.1 THE PROBLEM OF BIG DATA

To get at the answer to that question, one must start by acknowledging that Big Data is a real phenomenon, without doubt. Internet firms collect a lot of data about their users.[5] Every time we buy something on Amazon, the firm keeps a record of that purchase. Every time we engage in a Google search, Google tracks the subject matter. Every time we use Gmail to send an email, Google scans and records the content. And every time we post on Facebook, Facebook records the content. Especially for ubiquitous companies such as Google, the information recorded about individuals can be so extensive as to permit the firm to create a robust picture of the lives of particular people. Furthermore, if firms share data with each other, as they sometimes do,[6] they can develop even more extensive pictures of individual lives.

Of course, the problem of information collection and use, or more broadly what Zuboff terms "surveillance capitalism," is not limited to social media platforms, or even internet firms. Home devices such as Nest thermostats, home hubs, and security systems (Nest is owned by Alphabet, Google's parent

[5] Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. Davis L. Rev. 1183, 1187–94 (2016); *see also* Lina M. Khan and David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 Harv. L. Rev. 497, 498–502 (2019) (agreeing with Balkin about the reality of data practices and privacy concerns, but raising doubts about Balkin's proposed solution to the problem).

[6] *Your Data Is Shared and Sold … What's Being Done about It?*, Knowledge@Wharton (Oct. 28, 2019), https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 09 Nov 2026 at 06:00:40, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009547703.004

company[7]), as well as Amazon's "Echo" line of home hubs (and the smart assistant, Alexa, built into them), engage in what is in practice ubiquitous surveillance. And in this data age, even most brick-and-mortar stores, including such ubiquitous institutions as Safeway (an American grocery chain) and CVS (an American pharmacy chain), incentivize customers to open and use accounts which track all of their purchases. Furthermore, there exists a robust data brokerage industry in the United States and around the world, involving firms who collect vast amounts of data on individuals and sell it to any willing buyer (in 2024 that market is estimated to be worth $400 billion worldwide).[8] But there can be no doubt that internet platforms – notably Alphabet/Google and the social media giants – have perfected the ability to track clicks and likes to develop user profiles like nobody else, which is why their targeted advertising is so strikingly, and creepily, on target.

The reason why platforms have perfected data gathering and use is of course that, unlike brick-and-mortar stores or even home devices, Big Data is not peripheral to their business model; it is utterly central. The key point to understand is that especially for advertising-driven firms, such as Google and social media platforms, users are not the customers – we are the product. And for them to maximize their profits, they must serve their actual customers – the purchasers of online advertising – the precise (or as precise as possible) product that they want. So, if I perform a Google search for best mattresses, lo and behold, my online feeds become filled with mattress ads. Or (more optimistically) after I upload a social media post about planned travel to Italy, hotel and airfare ads show up everywhere.

The basic ways in which online advertising works are, of course, well known. But the significance of this for platform business models is well illustrated by a relatively recent sequence of events. In April of 2021, Apple announced a new privacy feature in the latest version of its operating system for iPhones, which would permit users to block apps from tracking users' behavior on websites and other apps (or more accurately, it required apps to gain consent, which was rarely forthcoming, from users before engaging in tracking).[9] In the past, firms such as Facebook had used tracking information to improve their targeted advertising. This new feature did not, of course,

[7] Eric Rosenbaum and Aashna Shah, *Nest Labs: How iPod Creator's Smart Thermostat Became a Top Google Brand*, CNBC (July 21, 2022), www.cnbc.com/2022/07/21/nest-labs-how-ipod-creators-thermostat-became-a-top-google-brand.html.

[8] www.knowledge-sourcing.com/report/global-data-broker-market.

[9] Alison DeNisco Rayome, *Protect Your Privacy By Disabling This App-Tracking iPhone Setting*, CNET (May 31, 2024), www.cnet.com/tech/services-and-software/protect-your-privacy-by-disabling-this-app-tracking-apple-iphone-setting/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 09 Nov 2026 at 06:00:40, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009547703.004

block targeted advertising; it merely reduced the amount of data available to personalize it. Nor did the privacy feature directly impact users' experiences on social media platforms. And finally, because this was an Apple feature, it also had no impact on tracking on Android phones. Nonetheless, in early 2022 Facebook announced that it expected Apple's new privacy policy to reduce its 2022 revenues by $10 *billion*. This announcement in turn contributed to a 26 percent drop in the share price of Meta, Facebook's (and Instagram's) parent company.[10] Other social media platforms faced similar drops in stock price, though in the long term Facebook, the platform most dependent on targeted advertising, seems to have been the biggest loser.

3.2 THE THREAT TO PRIVACY

Why does all of this matter? It matters because the harms associated with data collection and tracking are significant but, given the economic model of most social media platforms, there is little or no chance that the platforms will voluntarily cease or reduce their data collection practices. This is why the European Union and California have adopted privacy regulations, and why there have been continuous (albeit to date unsuccessful) proposals in the United States Congress to adopt a sweeping privacy-protection law. The wisdom, efficacy, and implications of such regulation are the topic of Chapter 7, so for now we will focus on the personal and social harms associated with Big Data.[11]

The most obvious risk associated with the widespread collection and storage of data is, of course, public leaks of personal information. Such leaks might be of embarrassing information about past conduct, which can take a wide variety of forms from infidelity to dishonesty to past crimes. A particularly extreme, intrusive, and troubling example of such leaks is sexually explicit photographs or videos, such as the 2014 release of nude photos of actress Jennifer Lawrence (which had been hacked from her iCloud account).[12] Such invasions of privacy can not only cause reputational harm but can also impose significant psychological trauma and interfere with future economic prospects (even if in utterly irrational and unjustifiable ways, as with the leak of intimate images).

[10] Meghan Bobrowsky, *Facebook Feels $10 Billion Sting from Apple's Privacy Push*, Wall Street Journal (Feb. 3, 2022), www.wsj.com/articles/facebook-feels-10-billion-sting-from-apples-privacy-push-11643898139.

[11] For a broad discussion of the value of privacy, *see* Neil Richards, Why Privacy Matters (2021).

[12] Laura M. Holson, *Hacker of Nude Photos of Jennifer Lawrence Gets 8 Months in Prison*, N.Y. Times (Aug. 30, 2018), www.nytimes.com/2018/08/30/arts/hack-jennifer-lawrence-guilty.html.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 09 Nov 2026 at 06:00:40, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009547703.004

Other sorts of information leaks can cause more direct, financial, or even physical harm to affected individuals. Leaked social security numbers can lead to identity theft. Leaked credit card or bank information can produce financial theft. Leaked home addresses can enable stalking or other physically threatening behavior. Indeed, leaks can be harmful even if they reveal no truly sensitive information, because public awareness of information such as an individual's political preferences or even reading habits can have significant social repercussions in our highly polarized and geographically politicized society. Woe betide a Republican in Berkeley, California, or a Democrat in Lafayette, Louisiana.

Of course, it is true that internet firms, including especially social media platforms, are quite unlikely to deliberately leak private user data or information to the general public. After all, any public release is likely to harm their relationships with users, with no offsetting benefits. Nor are the major, advertising-driven platforms likely to even sell user data to others. This data, after all, is not just financially valuable to them but the driving force of their profit model. As such, they are hardly likely to share it with potential competitors – and, in fact, both Facebook and Twitter/X explicitly state that they do not sell user data.[13]

Nevertheless, the very *existence* of large amounts of data stored on company servers makes leaks more likely, even if a leak requires bad actors to take advantage of the vulnerability of the stored data. But in the modern world, such bad actors are readily at hand, given the potential financial rewards from mining stolen data. In addition, hacking operations associated with state actors such as Russia[14] and China[15] also pose a constant threat to personal data, albeit the motivations there are less financial in nature (but no less potentially harmful).

Furthermore, even though internet firms are unlikely to engage in broad-based public disclosures of personal data, there are sound reasons to be concerned that they might leak intimate or embarrassing information about critics in order to discredit them, or threaten such leaks to silence critics or perceived enemies. Consider, for example, reports that in 2014 a senior Uber executive tracked the rides of a journalist, and a second senior executive floated a bizarre plan to use such tracking to dig dirt on journalists

[13] *Does Facebook Sell My Information?*, Facebook Help Center, www.facebook.com/help/152637448140583; *X Privacy Policy* ¶ 6.1 (Sept. 29, 2023), https://x.com/en/privacy#.

[14] Eileen Sullivan, *U.S. Disrupts Hacking Operation Led by Russian Intelligence*, N.Y. Times (Feb. 15, 2024), www.nytimes.com/2024/02/15/us/politics/hacking-russian-intelligence-routers.html.

[15] J. Edward Moreno, *China's Hacker Network: What to Know*, N.Y. Times (Feb. 22, 2024), www.nytimes.com/2024/02/22/business/china-hack-leak-isoon.html#.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 09 Nov 2026 at 06:00:40, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009547703.004

who criticize the company (in 2014, there were a lot of such journalists).[16] Uber immediately disclaimed these actions and instituted an internal privacy policy; but there can be no confidence that leaders of a firm facing strong public criticism will not be tempted to act similarly in the future. Consider also the fact that in December of 2022 TikTok confirmed that employees of TikTok's Chinese parent company, ByteDance, accessed the user data of two journalists in the course of investigating leaks.[17] The TikTok disclosure was particularly troubling because of concerns that the government of China, which has broad powers over even private Chinese firms such as ByteDance, might access user data for geopolitical reasons. Indeed, the disclosure as well as other long-standing concerns have resulted in numerous restrictions being placed on TikTok. Many countries have prohibited downloading TikTok onto government-issued phones, and India (as well, bizarrely, as the State of Montana) has flatly banned TikTok based on such concerns.[18] All of this culminated in federal legislation in the US that will ban TikTok if ByteDance does not divest its ownership interest in it (as of this writing, it remains unclear whether ByteDance will divest its ownership of TikTok, or whether TikTok will shut down in the US).[19]

Leaving aside leaks, threats of leaks, or misuse of information, even the seemingly legitimate use of personal data such as targeted advertising raises troubling possibilities. At first, targeted advertising of goods and services seems at most annoying, and sometimes useful. But personal information can be

[16] Alex Hern, *Uber Investigates Top Executive after Journalist's Privacy Was Breached*, The Guardian (Nov. 19, 2014), www.theguardian.com/technology/2014/nov/19/uber-investigates-top-executive-after-journalists-privacy-was-breached; Neil Irwin, *Uber Scandal Highlights Silicon Valley's Grown-Up Problem*, N.Y. Times (Nov. 19, 2014), www.nytimes.com/2014/11/20/upshot/ubers-latest-scandal-and-silicon-valleys-grown-up-problem.html.

[17] Clare Duffy, *TikTok Confirms that Journalists' Data Was Accessed by Employees of Its Parent Company*, CNN (Dec. 22, 2022), www.cnn.com/2022/12/22/tech/tiktok-bytedance-journalist-data/index.html.

[18] Kelvin Chan, *Here Are the Countries That Have Bans on TikTok*, AP News (April 4, 2023), https://apnews.com/article/tiktok-ban-privacy-cybersecurity-bytedance-china-2dce297f0aed056efe53309bbcd44a04; https://news.mt.gov/Governors-Office/Governor_Gianforte_Bans_TikTok_in_Montana.

[19] Sapna Maheshwari and Amanda Holpuch, *Why the U.S. Is Forcing TikTok to Be Sold or Banned*, N.Y. Times (June 20, 2024), www.nytimes.com/article/tiktok-ban.html. In January of 2025 the US Supreme Court rejected constitutional challenges to the TikTok law. TikTok Inc. v. Garland, 145 S. Ct. 57 (2025) (per curiam) (full disclosure – I participated in an amicus brief in the litigation over the TikTok law, supporting TikTok's position that the law violates the First Amendment). Subsequently, however, President Trump issued an Executive Order suspending enforcement of the law against TikTok. *Application of Protecting Americans from Foreign Adversary Controlled Applications Act to TikTok* (Jan. 20, 2025), www.whitehouse.gov/presidential-actions/2025/01/application-of-protecting-americans-from-foreign-adversary-controlled-applications-act-to-tiktok/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 09 Nov 2026 at 06:00:40, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009547703.004

used to influence and manipulate choices beyond the commercial sphere. As Professors Jack Balkin of the Yale Law School and Jonathan Zittrain of the Harvard Law School recount, during the 2010 midterm election Facebook conducted an experiment in which it added graphics to some users' news feeds that were designed to encourage them to vote.[20] The impact of this post was small (targeted users were 0.39 percent more likely to vote), but given Facebook's enormous user base, that can translate into a lot of votes, potentially enough to swing a close election. The risk, of course, is that because Facebook can pretty reliably predict users' political inclinations based on their personal data, it could manipulate election results by encouraging turnout only of voters of a particular political persuasion.[21] Which is not to say that Facebook, or any other platform, has actually engaged in such behavior, but this possibility poses a rather more serious problem than a consumer being convinced to buy a pair of shoes they do not need. And given Elon Musk's almost-simultaneous takeover of Twitter/X, and embracing his role as a rabid Republican supporter of Donald Trump,[22] the risks of such (mis)conduct are not farfetched.

As Shoshana Zuboff nicely describes it, the basic problem, the social risk, posed by "surveillance capitalism," which is to say the collecting and processing of massive amounts of personal data, implicates the very nature of our society. In the modern digital economy, information about human experience (i.e., personal data) is the key input into a huge amount of economic activity. The result is that those who possess and control that data, primarily the major technology companies such as Alphabet (owner of Google and YouTube), Meta (owner of Facebook, Instagram, and WhatsApp), and Amazon have the power to predict and manipulate a huge range of human choices. Their primary motivations in doing so are, of course, commercial; surveillance capitalism is, after all, *capitalism*. But as noted earlier, the power to extend such manipulation and control into social and political spheres certainly exists. Furthermore, because the tech sector is highly concentrated and (unlike the manufacturing firms that dominated earlier versions of capitalism) tends to employ relatively small numbers of highly educated people, the concentration of power entailed by this system is far more dramatic than in earlier eras.[23] Indeed, as of 2024

[20] Balkin, *supra* n. 5, at 1188–89 (internal citation omitted); *see* Jonathan Zittrain, *Facebook Could Decide an Election without Anyone Ever Finding Out*, New Republic (June 1, 2014), www.newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering.

[21] Jonathan Zittrain, Response, *Engineering an Election*, 127 Harv. L. Rev. F. 335, 336 (2014).

[22] Theodore Schleifer, Maggie Haberman, Ryan Mac, and Jonathan Swift, *Musk Is Going All in to Elect Trump*, N.Y. Times (Oct. 11, 2024), www.nytimes.com/2024/10/11/us/politics/elon-musk-donald-trump-pennsylvania.html.

[23] *Surveillance Capitalism*, *supra* n. 1, at 500–01.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 09 Nov 2026 at 06:00:40, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009547703.004

just a handful of individuals – Elon Musk, Mark Zuckerberg, and Jeff Bezos, notably – exercise complete control over many of the tech giants. As such, it can be argued that the rise of Big Data has fundamentally altered the structure of our societies, making them less democratic and in some sense less free.

3.3 COUNTER CONSIDERATIONS

There is, in short, no serious doubt that we live in a society and economy in which massive amounts of personal data collection and storage occur on a continuous and ongoing basis. There is also no serious doubt that personal data can be easily misused, and that even the possibility of accidental data leaks raises real privacy concerns. If one takes commentators and the media seriously, it is easy to come to the conclusion that the combination of Big Data and the death of privacy imposes constant harms on many people and threatens to change the very nature of our society. But to what extent are these extreme warning cries justified?

The scale of the risks posed by the data practices of modern platforms (and others) is honestly difficult to determine accurately, but there are reasons to believe the risks are somewhat exaggerated. Consider, for example, the concern that personal data will be misused by firms to target enemies and critics. That such a risk exists is certainly true, as demonstrated by the Uber and TikTok revelations. But in both cases the incidents appear to have been isolated ones, which were quickly rectified, and there is certainly no evidence that firms routinely misuse data in this way.

For example, when Montana's Governor Greg Gianforte signed a bill in May of 2023 completely banning TikTok within the state, he cited privacy concerns raised by the fact that TikTok's owner, ByteDance, is a Chinese company. The governor's release stated that the "Chinese Communist Party using TikTok to spy on Americans, violate our privacy, and collect their personal, private, and sensitive information is well-documented."[24] But tellingly, neither the governor nor the legislature could point to any evidence to support this claim, and TikTok insists that it has never shared US user data with the Chinese government or Communist Party.[25] Moreover, cybersecurity experts appear to support TikTok's position, rather than Governor Gianforte's

[24] *Governor Gianforte Bans TikTok in Montana*, STATE OF MONT. (May 17, 2023), https://news.mt.gov/Governors-Office/Governor_Gianforte_Bans_TikTok_in_Montana.

[25] David Shepardson, *TikTok CEO: App Has Never Shared US Data with Chinese Government*, REUTERS (March 21, 2023), www.reuters.com/technology/tiktok-ceo-app-has-never-shared-us-data-with-chinese-goverment-2023-03-22/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 09 Nov 2026 at 06:00:40, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009547703.004

unsupported claims.[26] This is not to say, of course, that there is *no* risk that the Chinese government, not known for its concerns about privacy or civil liberties, would coerce TikTok to share data – which is why ongoing pressure on TikTok to store US user data in the US makes sense.[27] But it seems equally clear that public statements by politicians and in the media about TikTok are greatly exaggerated and that TikTok bans, such as the Montana and federal laws, appear to be driven more by anti-China political sentiment than empirically grounded concerns.

Now consider the problem of leaks. Again, there can be little doubt that data leaks happen, as illustrated by the Facebook/Cambridge Analytica fiasco.[28] But how often do these leaks involve truly personal or private, potentially embarrassing, or weaponizable information, as opposed to information which can be harmful if public but otherwise lacking any moral valence, such as social security or credit card numbers? Of course, even the release of information that can be used to steal money or identity is harmful. But for one thing, social media platforms (as opposed to sellers of goods such as Amazon) are relatively unlikely to possess that sort of financial information. Furthermore, leaks of financial information (which, after all, long predate the internet) do not threaten basic societal stability or structures. It is when information can be used to generate social and political power that serious concerns arise.

So, it is worth asking again, how often do data leaks occur which raise such fundamental concerns? As is so often the case, there can be no definitive answer to that question, but all indications are that such events are exceedingly rare. They do of course happen, a prime example being the leak of intimate photos of Jennifer Lawrence and others. But they are not a recurring or common occurrence. None of which is to excuse leaks when they occur, of course, or to reduce the need for those who control data to secure it. But when considering appropriate regulatory initiatives, it is important to ensure that they are proportionate to the underlying problem, because even privacy regulation inevitably has unintended or negative consequences (as discussed further in Chapter 7).

One further point here: The fact that leaks of weaponizable data collected by platforms is rare does *not* mean that third parties/users have not utilized

[26] Max Zahn, *No Evidence of TikTok National Security Threat but Reason for Concern, Experts Say*, ABC News (March 28, 2023), https://abcnews.go.com/Technology/evidence-tiktok-national-security-threat-reason-concern-experts/story?id=98149650#.

[27] Echo Wang and David Shepardson, *TikTok Moves U.S. User Data to Oracle Servers*, Reuters (June 17, 2022), www.reuters.com/technology/tiktok-moves-us-user-data-oracle-servers-2022-06-17/.

[28] Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, N.Y. Times (April 4, 2018), www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 09 Nov 2026 at 06:00:40, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009547703.004

the internet and platforms to expose and circulate personal information in extremely harmful ways. As discussed in Chapter 2, doxing and the like are troublingly common phenomena. And in the most repulsive such instances, such as sharing nonconsensual intimate images, such propagation can cause extreme, personal harm. The point is, however, that none of these sorts of abuses can be tied to the data collection, storage, and use policies of the big platforms. They instead are a product of bad actors and, on the platforms' part, (arguable) failures of content moderation. In Chapter 8, we will consider possible regulatory responses to this problem; but traditional privacy rules, directed at data practices, are not among them.

Finally, let us consider the risk that platforms (and other owners of large databases) will use the data not to target enemies but to manipulate society as a whole. An example of such behavior was Facebook's experiment during the 2010 election, described earlier, seeking to enhance voter turnout. While Facebook's conduct there was innocuous, as noted earlier similar actions could be used in highly disquieting ways, such as to try and push elections in particular directions. That such manipulation is possible is clear. Further, the extreme concentration of ownership of the major social media platforms – Mark Zuckerberg and Elon Musk, alone, each have dominant positions – makes the possibility greater because it is easier to imagine an individual pursuing such political games than publicly traded companies. Indeed, Musk's increasing politicization is particularly concerning in this regard, as illustrated by claims, admittedly unproven, that in the summer of 2024, Twitter/X interfered with the social media activities of groups supporting Democratic presidential candidate Kamala Harris.[29] But there are also disincentives to such behavior, most obviously that public disclosure of any such attempts would be a public relations disaster. And given that employees of platform companies would have to be aware of, and aid in implementing, such a scheme, ultimate disclosure would be highly likely (if it was not publicly visible, as with Twitter/X's suspension of the pro-Harris account). And lastly, as the Facebook example shows, attempts to use nudges or posts to manipulate conduct appear to have at best marginal effects.

One might ask, however, what the harm is in sharply restricting the data practices of big platforms (as, to some extent, the European Union is doing). After all, the accumulation of small risks can add up to significant ones, so why not act? The short answer is that, while some regulation might be justified,

[29] Trisha Thadani, Will Oremus, and Eva Dou, *X Suspends "White Dudes for Harris" Account after Massive Fundraiser*, Washington Post (July 31, 2024), www.washingtonpost.com/technology/2024/07/30/white-dudes-harris-suspended-x-twitter/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 09 Nov 2026 at 06:00:40, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009547703.004

there are serious downsides to regulation. What those downsides are, and what effective regulation might look like, are the topics of Chapter 7, but for now let us touch upon two.

The first, in brief, is that data collection and use is at the heart of the business models of the major current platforms. That is how they make money. To interfere with that model is to interfere with lucrative economic activity, which itself is problematic in a free market economy (it is no coincidence, in this regard, that the targets of the European Union's regulatory initiatives are almost exclusively US companies, and so have little impact on European companies and profits). But in addition, it is the data/advertising business model that permits platforms to offer their services to users without charge. Eliminate the business model, and the free services will either entirely disappear, or will no longer be free.

Second, it is important to remember that information is speech. To stop the collection and distribution of information is, therefore, definitionally an interference with free speech. This is not to say that restrictions are never permissible – free speech rights are not, after all, absolute. But regulations do raise serious constitutional and political concerns, and so must be considered with care – as we shall do in Chapter 7.

To conclude, the data practices of the major social media platforms undoubtedly threaten serious privacy and other social harms. At the same time, the scale and seriousness of such harms have almost certainly been exaggerated in public debate and criticisms of platforms. Finally, regulation itself threatens serious social and legal harms to users, and to society. Careful consideration and balancing of the harms is therefore essential before sweeping regulatory initiatives are undertaken.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 09 Nov 2026 at 06:00:40, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009547703.004