8

Some Ways Forward

To this point, this book has been in many ways an extended disquisition on why many contemporary critiques of social media are flawed or exaggerated, and why many reform proposals directed at social media are misguided. But this book is not meant to be a plea for either complacence or inaction. After all, to say that the war on social media consists to a significant degree of hyperbole and evidence-free innuendo is *not* to say that social media does not create any social harms worthy of a regulatory response.

8.1 FIRST, DO NO HARM: PERVERSE INCENTIVES AND CONSTANT CHANGE

Having acknowledged the existence of harms associated with social media, I would nonetheless argue that the default assumption should be against rather than, as the European Union (EU) increasingly appears to believe, for regulations directed specifically at social media (or for that matter other new technologies). In other words, would-be regulators of new technologies should adopt the principle of medical ethics attributed (somewhat incorrectly) to the ancient Greek physician Hippocrates: *primum non nocere*, or "First, do no harm." And while the relevance of this principle for modern medicine is highly debatable,[1] it made all sorts of sense in premodern times, when medical interventions were incredibly dangerous (especially because of the risk of infection, in a pre-antibiotics age) and rooted in deep ignorance about the basic science of human health. So it is with social media today.

Digging deeper, the reasons why it makes sense to adopt the "do no harm" principle for social media are straightforward. Foremost is simply that social

[1] Robert H. Shmerling, MD, *First Do No Harm*, Harvard Health Blog (June 22, 2020), www.health.harvard.edu/blog/first-do-no-harm-201510138421.

media is *media*, and regulations of social media are regulations of speech. Furthermore, as the US Supreme Court has recognized, social media is today the primary locus for broad discussions of public issues.[2] But in the United States under its First Amendment, the presumption has always been against government intervention in public discourse. Indeed, the same should be true in any free and democratic society committed to open debate. Why that is so follows from first principles. Free Speech is widely accepted as an essential element of any democratic system of government; and at least in the United States the primary reason why the First Amendment protects expressive freedoms is to advance democratic self-governance.[3] From this follows an important, if controversial, principle: Government, and government regulation in particular, is always and foremost the gravest threat to freedom of expression. This is true for two separate reasons.

First, unlike private actors, government actors have systematically perverse incentives when regulating public discourse. Elected officials, of course, wish to stay in power, and unelected officials need to maintain the support of elected officials to sustain their authority. But the greatest threat to retaining power is public discourse about elected officials' conduct in office, which can reveal their errors, weaknesses, and malfeasance, and so turn voters against them. As such, government regulators are *always* motivated to reshape or suppress public discourse, especially discourse about the government itself. Of course, not all officials act on these perverse motivations; but nonetheless, perhaps the primary purpose of constitutional protections for free expression is to create barriers to such manipulation of discourse.

It should be noted in this regard that while, as Chapter 1 recounts, numerous (mainly conservative) critics of social media accuse platforms of similar censorial motives, this does not make much sense. In fact, at heart the goal of social media firms is to *maximize* speech, because that is in some sense the product they are providing. To be more precise, platforms host speech to attract users, and then make money by selling access to those users to advertisers. Platforms cannot adopt aggressive rules restricting content because their financial goal is to maximize users; and to maximize users they need to maximize the speech that attracts them. And from the point of view of the platform, it is entirely irrelevant if the speech they host is favorable to the government, unfavorable to the government, or has nothing to do with government – the more the merrier. Indeed, even content which is unpopular with the majority

[2] Packingham v. North Carolina, 582 U.S. 98, 104 (2017).

[3] I explore these themes in detail in Ashutosh Bhagwat, Our Democratic First Amendment (2020).

of users typically is of interest to some elements of the population, and so, to maximize users, platforms are incentivized to permit that speech. Only when speech is so unpopular with a significant percentage of users that it is likely to scare them away will it benefit platforms to suppress it.

Second, and more fundamentally, for all the wealth and power that owners of social media platforms such as Mark Zuckerberg and Elon Musk possess, governments continue to enjoy a monopoly on legal violence. While tech moguls can ban certain words, and even ideas, from their platforms (for example, as of this writing Elon Musk has apparently banned the terms "cis" and "cisgender" from Twitter/X[4]), they cannot arrest you, lock you up, physically harm you, or even take your property against your will. In contrast, violations of legal regimes such as Germany's NetzDG, as well as India's IT Act and implementing rules (both discussed in Chapter 6), subject platforms to sometimes whopping fines, as well as the potential imprisonment of platform employees. NetzDG, for example, authorizes fines of up to 50 *million euros*,[5] and Section 69A(3) of the Indian IT Act of 2000 authorizes imprisonment for up to *seven years* for violations of that section.[6] This kind of coercive authority can silence and deter speech in ways that simply cannot be matched by the inconvenience of having a post blocked, or even being deplatformed, by Facebook or Twitter/X.

Furthermore, even though powerful platforms are sometimes loosely described as "monopolies," they certainly do not possess the monopolistic control mechanisms enjoyed by the state. Elon Musk may try to ban the term "cis" on Twitter/X, but other platforms do not. And even if the very large platforms all ban particular expression such as hate speech, alternative platforms such as Telegram remain available.[7] State power, on the other hand, is pervasive and omnipresent. When Germany bans Nazi propaganda via its NetzDG law, such speech is entirely excluded from the county. Consider in this regard the fact that in early September of 2024 the supreme court of Brazil completely banned the platform Twitter/X from the country (affirming a previous decision by a single justice), because of the platform's failure to comply

4 Siladitya Ray, *Musk Says "Cisgender" and "Cis" Are Now "Slurs" on Twitter*, FORBES (June 21, 2023), www.forbes.com/sites/siladityaray/2023/06/21/musk-says-cisgender-and-cis-are-now-slurs-on-twitter/.

5 *Germany Starts Enforcing Hate Speech Law*, BBC (Jan. 1, 2018), www.bbc.com/news/technology-42510868.

6 Information Technology Act, 2000.

7 Though apparently not without legal consequences, at least in Europe. *See* Aurelien Breeden, *What We Know about the Telegram Founder's Arrest*, N.Y. TIMES (Aug. 27, 2024), www.nytimes.com/2024/08/27/business/telegram-pavel-durov-arrest-explained.html (discussing arrest and charging in France of Telegram founder Pavel Durov based on illegal activity on Telegram).

with Brazilian law regarding illegal content.[8] Presumably other social media platforms will take heed and follow Brazilian law. No social media firm or owner, even Mark Zuckerberg (the effective owner of Facebook, Instagram, WhatsApp, and Threads), has that kind of power.

In short, both because of government's perverse motivations and because of its monopoly on legal violence, it is sensible to approach government regulation of social media with an attitude of heightened skepticism. But there is another, quite separate reason for such skepticism (and a presumption against regulation), analogous to premodern medicine: ignorance and unpredictability. And this in turn is tied to a phenomenon deeply associated with the internet and social media, which is constant change.

Let us begin with the fact that, as technologies go, social media itself is relatively new. Facebook did not become available to the general public until 2006,[9] the same year that Twitter/X was founded[10] and YouTube was purchased by Google (YouTube was founded the previous year).[11] Instagram was not launched until 2010 (and not purchased by Facebook/Meta until 2012).[12] And none of these platforms obtained their ubiquitous presence in society until smart phones gained mass usage in the early 2010s (the first iPhone was launched in 2007[13]). So modern attempts to regulate these platforms such as the EU's General Data Protection Regulation (GDPR) (which was written in 2016 and became effective in 2018)[14] began barely a decade after the primary modern social media platforms came into existence. To give a comparison, while the telephone was invented in the 1870s, the US Congress did not regulate it until 1910 and did not adopt an extensive telecommunications statute until 1934.[15]

[8] Tom Phillips, *Brazil's Supreme Court Upholds Ban on Elon Musk's X over "Illegal Conduct,"* The Guardian (Sept. 2, 2024), www.theguardian.com/technology/article/2024/sep/02/brazils-supreme-court-upholds-x-ban-over-conduct.

[9] Sarah Phillips, *A Brief History of Facebook*, The Guardian (July 25, 2007), www.theguardian.com/technology/2007/jul/25/media.newmedia.

[10] Jonathan Vanian, *Twitter Is Now Owned by Elon Musk: Here's a Brief History from the App's Founding in 2006 to the Present*, CNBC (Oct. 29, 2022), www.cnbc.com/2022/10/29/a-brief-history-of-twitter-from-its-founding-in-2006-to-musk-takeover.html.

[11] *Google Buys YouTube for $1.65 Billion*, NBC News (Oct. 9, 2006), www.nbcnews.com/id/wbna15196982.

[12] Allison Eldridge, *Instagram*, Britannica Money (Sept. 2, 2024), www.britannica.com/money/Instagram.

[13] Apple, www.apple.com/newsroom/2007/01/09Apple-Reinvents-the-Phone-with-iPhone/.

[14] General Data Protection Regulation 2016/679, 2016 O.J. (L 119), https://eur-lex.europa.eu/eli/reg/2016/679/oj (henceforth "GDPR").

[15] Tim Wu, *A Brief History of American Telecommunications Regulation*, 5 Oxford International Encyclopedia of Legal History 95 (2009), https://scholarship.law.columbia.edu/faculty_scholarship/1461.

But even more significantly than the relative youth of the technology, what is notable about the social media ecosphere is that it remains subject to constant change and flux. Consider that in 2016, when (primarily as a result of the Brexit and US presidential elections) close attention began to be paid to social media's societal consequences, it seemed clear that the largest of those platforms, Facebook, was destined to rise relentlessly. Yet in the United States, the percentage of adults who use Facebook has been almost flat since 2016, and among teenagers Facebook is *far* less popular than other platforms such as TikTok and Instagram.[16] Given its demographic challenges, therefore, the future of Facebook remains very murky.

TikTok presents an even more extreme example of flux. In 2016 TikTok was unknown. Yet TikTok has, in a few years, famously become by far the most popular platform among teenage and young adult users, in the United States and around the world. But TikTok's story continues to evolve. As of this writing (in the fall of 2024), there is a good chance that TikTok will be completely ejected from the United States pursuant to a congressional statute adopted in April of 2024, which will require TikTok to either separate from its Chinese parent, ByteDance, or stop operating in the United States.[17] And even if ByteDance does sell its stake in TikTok, the resulting platform will undoubtedly change with new ownership. Furthermore, TikTok has been banned in India, the world's most populous nation, since 2020.[18] So is TikTok, with its young user base, the future and so worthy of regulatory attention, or is it becoming irrelevant?

Or consider Twitter/X. Because so much political dialogue traditionally occurred on that platform, it was of special concern to would-be regulators (with all of their perverse incentives). President Trump, in particular, used Twitter/X as an official vehicle for policymaking during his first term as President, going so far as to fire his Secretary of Defense via Twitter/X.[19] It was almost certainly Twitter/X's deplatforming of Trump in January of 2021 that led Florida and Texas to enact the social media laws discussed in Chapter 1. Yet since Elon Musk's purchase and takeover of Twitter/X in October of

[16] Katherine Schaeffer, *5 Facts about How Americans Use Facebook, Two Decades after Its Launch*, Pew Research Center (Feb. 2, 2024), www.pewresearch.org/short-reads/2024/02/02/5-facts-about-how-americans-use-facebook-two-decades-after-its-launch/.

[17] Bobby Allyn, *President Biden Signs Law to Ban TikTok Nationwide Unless It Is Sold*, NPR (April 24, 2024), www.npr.org/2024/04/24/1246663779/biden-ban-tiktok-us.

[18] Alex Travelli and Suhasini Raj, *What Happened When India Pulled the Plug on TikTok*, N.Y. Times (March 22, 2024), www.nytimes.com/2024/03/22/business/tiktok-india-ban.html.

[19] Guy Snodgrass, *Trump Fires Secretary of Defense Mark Esper Via Tweet*, Forbes (Nov. 9, 2020), www.forbes.com/sites/guysnodgrass/2020/11/09/trump-fires-secretary-of-defense-mark-esper-via-tweet/.

2022, most of the conservative concerns and grievances directed at Twitter/X have become entirely moot. Indeed, it is now progressives who are moaning about Twitter/X, given Musk's public right-wing turn, which he is increasingly extending to his management of Twitter/X (recall his banning the words "cis" and "cisgender"). Furthermore, given Twitter/X's enormous financial difficulties in the wake of the Musk takeover, here too the present and the future are grossly uncertain.

Finally, there are many other, continuing evolutions that make it extremely difficult to predict the near, and especially more distant future of social media. Even Facebook, the granddaddy of the current platforms (in terms of age and user base), is constantly tweaking the algorithms that control its Feed, moving from personal to more commercial and political, and then sometimes back to more personal content. It has also come to emphasize reels over posts in its panic over the rise of TikTok (which may perhaps reverse if TikTok goes away). And most famously, Facebook has been extraordinarily inconsistent regarding its willingness to police false information, especially in the wake of the 2016 US election, and even more so the COVID-19 pandemic and lockdowns. In 2020, Mark Zuckerberg famously announced on air that "Facebook or internet platforms in general" should not be "arbiters of truth."[20] Yet it is now public knowledge (which Zuckerberg has acknowledged) that the following year Facebook, under heavy public and private pressure, cooperated extensively with the Biden Administration's efforts to suppress COVID and vaccine mis- and disinformation – something that Zuckerberg later said he regretted doing.[21]

One could go on at length in this vein, but the bottom line is clear: Social media is far from a mature technology and continues to demonstrate constant and fundamental change. But this fact alone creates serious problems for would-be regulators. Regulation, by its nature, is designed to address ongoing and future societal harms connected to the subject of regulation. Indeed, given the slow pace at which laws and regulations are adopted and implemented, in truth the main concern must be future, not present, harm. But in the face of such constant and fundamental change, how can regulators possibly predict what specific harms will be associated, several years down the line, with social media platforms? They of course cannot, making effective regulation

[20] Salvador Rodriguez, *Mark Zuckerberg Says Social Networks Should Not Be Fact-Checking Political Speech*, CNBC (May 28, 2020), www.cnbc.com/2020/05/28/zuckerberg-facebook-twitter-should-not-fact-check-political-speech.html.

[21] Gnaneshwar Rajan and Nandita Bose, *Zuckerberg Says Biden Administration Pressured Meta to Censor COVID-19 Content*, Reuters (Aug. 27, 2024), www.reuters.com/technology/zuckerberg-says-biden-administration-pressured-meta-censor-covid-19-content-2024-08-27/; Murthy v. Missouri, 144 S. Ct. 1972 (2024).

exceedingly hard to draft. One should thus be highly skeptical of social media regulation, and of regulators who claim to be able to predict the future.

Furthermore, it is not just that regulation has a high chance of failing; it can also have perverse effects. Regulation almost always imposes compliance costs, which ultimately will be borne by platform customers, whether users or advertisers. Those costs may well be justified if they are associated with benefits/harm preventions; but absent such benefits, regulation is hard to defend from the perspective of social welfare. In addition, regulation inevitably raises barriers to entry, especially for smaller, start-up potential entrants. But, given that excess concentration is (legitimately) one of the more serious criticisms leveled at the social media sphere, making it harder for entrants to challenge Big Tech incumbents is seriously misguided, unless there are strong, countervailing reason to do so. It may be easier for regulators to deal with only a handful of dominant platforms, but, for we-the-users, choice is better.

All of which is to say, regulation imposes social costs, which must be justified by social benefits. But in the face of change and uncertainty, it is hard to be sure that regulations will, over any reasonable time horizon, produce such benefits. And that is why skepticism and a presumption against new regulation targeting social media make sense.

8.2 ENFORCING EXISTING LAWS

That said, a presumption against new regulation targeting social media does *not* mean that social media should be a law-free zone. Most obviously (though the obviousness of this is sometimes lost), social media companies should be, and are, subject to long-standing, general legal rules. The rules and restrictions I speak of are broad and universal, are not focused on any particular industry or technology, and have stood the test of time. And they address broad societal concerns. As such, there is absolutely no reason why social media firms should get some sort of an exemption or pass from rules that everyone else must follow.

That social media firms must follow the law should be obvious, and in some respects it is entirely uncontested. Of course Meta, Twitter/X, Alphabet, and TikTok must pay their employees at least minimum wage, provide them with safe work environments, and permit non-exempt staff to unionize if they desire. And of course their headquarters must comply with local building codes and zoning laws. One could go on. No one seriously contests this point, but it is important to highlight it. The difficulty arises when such laws interfere with how platforms operate, at which point this consensus appears to vanish.

Take antitrust. The social media industry (and Big Tech more generally) is famously highly concentrated, and so seemingly rife for antitrust scrutiny. Yet

for years, antitrust regulators (inexplicably) took a largely hands-off approach, presumably because of concerns about throttling a new and exciting technology. Thus when, early in its existence, Facebook went on a buying spree, purchasing Instagram (a direct competitor) in 2012, and then WhatsApp (seen as a potential competitor) in 2014, the deals were waived through with almost no regulatory scrutiny. It is entirely possible that part of the reason for this was that, at the time, regulators did not fully understand the nature of the social media industry, since on the surface it would seem as if these companies were simply giving away their services for free. But if so, that naivete is surely a thing of the past as we now understand that platforms' true customers are advertisers – users are merely an input into their business model. None of which is to say that Facebook's acquisitions *did* violate antitrust law; but they should not have gotten the free pass that they apparently did at the time. And, it should be added, the same can be said of Google's acquisition of YouTube in 2006 – search and online videos may seem like different industries, but both firms are in the business of selling online advertising and so should have been seen as competitors.

Nor is the failure to scrutinize mergers the only area where regulators may have failed to apply antitrust principles to platforms. Consider, for example, Meta's tendency to introduce new platforms or features to challenge and undermine rivals, such as Instagram stories for Snapchat and Threads for Twitter/X. Such conduct in and of itself does not raise any antitrust (or other) concerns; to the contrary, it probably represents healthy competition. But if Meta were to use its dominance on one platform to leverage competitive advantages into other forms of social media, that *would* be potentially problematic. This is not to say that Meta *has* engaged in such anticompetitive conduct; but certainly, greater attention to such possibilities than regulators have to date given seems in order.

In recent years, fortunately, a bipartisan consensus appears to have been reached among regulators that antitrust law should apply to Big Tech just as to any other industry. Regarding social media platforms in particular, in 2020 (during the first Trump Administration) the Federal Trade Commission (FTC) filed a lawsuit seeking to reverse Facebook's acquisition of Instagram and WhatsApp, potentially requiring Meta to divest itself of both platforms. The Biden Administration FTC has continued the lawsuit, which as of this writing (Fall 2024) is still ongoing.[22] Seen in light of other recently launched lawsuits targeting Google, Amazon, and Apple, these developments suggest

[22] Cecelia Kang, *A Facebook Antitrust Suit Can Move Forward, a Judge Says, in a Win for the F.T.C.*, N.Y. Times (Jan. 11, 2022), www.nytimes.com/2022/01/11/technology/facebook-antitrust-ftc.html.

that Big Tech's days of freedom from antitrust scrutiny are over. And that is a good thing.

Another body of law that has obvious relevance to the operation of social media platforms is contract law. The basic premise of contract law is blindingly simple: When parties enter into a legally binding agreement, they are responsible for sticking to the terms of that agreement. When social media platforms offer services to users under certain terms and conditions, including content moderation standards, they and the users are entering into a contract. It may seem as if that is not true because platforms do not charge users (i.e., in technical legal terms that there is no "consideration" from users for the services), but that is not actually the case. The "deal" with respect to social media is that platforms offer services in exchange for their users' data and eyeballs, which platforms in turn use to generate advertising revenues.

Why does this matter? Because contracts are *mutually* binding. Just as platforms are entitled to block content or users that violate their terms of service, just so platforms have a legal obligation to users to themselves follow those terms. If they fail to do so, platforms can and should be held legally liable. Admittedly, it is bit unclear what exactly the legal remedy should be when a platform acts contrary to its own terms of service (money damages seem an odd fit, given that users do not pay platforms); but one can imagine inventive jurists finding *some* means to incentivize platforms to play by their own rules, including perhaps judicial injunctions (which are not a standard remedy in breach of contract cases).

Furthermore, the law imposes various restrictions on what terms may be included in contracts. For example, contractual terms may not be "unconscionable," meaning grossly unfair in how the term is imposed on one party and in its substantive effect. Given platforms' essentially unlimited power to set terms of use, the first element is surely satisfied, meaning that courts can and should be entitled to set aside grossly unfair terms of service, at the behest of users or regulators. Similarly, contract law, as well as related consumer protection statutes, provide tools to police misleading terms of service adopted by platforms, in the same way that other industries are forbidden from deceiving customers. And one could go on. The main point is that plain old contract law, perhaps as foundational and un-innovative a body of law as there is, can be a source of many important constraints on platforms.

Another basic and long-standing body of law that can and should, when appropriate, be applied against platforms is tort law. Of course, Section 230 precludes tort liability for third-party content on platforms (on which more later) or for good faith content moderation decisions. But as discussed in detail in Chapter 6, Section 230 does *not* shield platforms from liability for harm

caused by design features built into the platforms. This is why the case based on Snapchat's "Speed Filter" could proceed despite Section 230. And this is also why a federal judge in Oakland has permitted parts of a lawsuit brought by school districts against major platforms to proceed (both cases are discussed in Chapter 6).

Also on the topic of tort law, and as also discussed in Chapter 6, serious uncertainty exists about whether Section 230 shields platforms from liability for harm caused by their recommendation algorithms. Some courts (including the judge in the Oakland school district litigation) have said that it does provide such immunity. But other courts have disagreed. In particular, in an important opinion issued in August of 2024, the United States Court of Appeals for the Third Circuit (which covers the mid-Atlantic states), so held.[23] This extremely disturbing case involved a video on TikTok depicting the "Blackout Challenge," which encouraged users to try and make themselves pass out. TikTok's algorithm recommended this video to a 10-year-old child, who ended up dying when she attempted to perform the challenge. The court, reversing a lower court decision, permitted a lawsuit brought by the girl's mother to proceed insofar as it was based on TikTok's recommendation algorithm rather than the content itself. And interestingly, in reaching this conclusion the Third Circuit majority relied heavily on the fact that in its *NetChoice* decision (discussed in detail in Chapter 4), the Supreme Court held that content curation by platforms was protected by the First Amendment. That, the Third Circuit concluded, meant that recommendations were *not* the same as the underlying third-party content, and so fell outside Section 230.

In other words, courts are currently working through many issues regarding how long-standing legal principles, including antitrust, contract, and tort law, apply to modern platforms. And while some questions, such as Section 230's application to recommendation algorithms, remain very much in flux, others, such as the obligation on platforms, just like everyone else, to follow general legal rules, are not. But regardless of how specific issues are resolved, what is very clear is that the space in which social media platforms operate is very much *not* a "law-free" zone.

Finally, if antitrust, contract, and tort law are obvious sources of rules governing platforms, there also exist some other, non-obvious but potentially important legal restrictions. One of those, surprisingly, may be family law. In a very interesting paper, law professor Katharine Silbaugh and her then

[23] Anderson v. TikTok, Inc., 116 F.4th 180 (3rd Cir. 2024); David French, *The Viral Blackout Challenge is Killing Young People. Courts Are Finally Taking It Seriously*, N.Y. Times (Sept. 5, 2024), www.nytimes.com/2024/09/05/opinion/tiktok-blackout-challenge-anderson.html.

student Adi Caplan-Bicker argue that family law provides a completely overlooked tool to combat children's exposure to harmful content on social media platforms.[24]

To simplify a complex and thoughtful argument, Silbaugh and Caplan-Baker argue that instead of directly targeting online content that regulators view as harmful, which the First Amendment and Section 230 generally do not permit, regulators should enact consent-based laws which empower parents to opt their children in or out of social media platforms but do not focus on specific types of content. Most intriguingly, they propose creating a central "Parental Decision-Making Registry," on which parents could register their preferences regarding their children's social media access, at a device level. Such a registry could permit parents to simply opt their children out of social media, in which case platforms would be required to comply. But they could also opt into less restrictive limitations, such as a social media curfew. And most importantly, Sibaugh and Caplan-Baker argue that such restrictions, so long as they were content-neutral, are consistent with current First Amendment law.

There is a basic insight underlying this clever proposal. It is largely none of the government's business what types of legal content are accessed by individuals, including minors (especially teenagers). And even when a law is designed to enhance parental authority rather than flatly ban access to specific content by minors, it is presumptively impermissible for the government to single out specific content for regulation. This was the basic, and correct, lesson of an important Supreme Court case invalidating a California law restricting the sale of violent video games to minors.[25] On the other hand, it is a fundamental principle of family law, going back untold centuries, that it is very much the business of parents to control their children's upbringing, including their education and their exposure to different perspectives and information.[26] Indeed, in two decisions from the 1920s that are still followed, the Supreme Court held that parents had a constitutional *right* to control their children's education.[27] And that right surely extends to children's access to information in a non-school setting, including on social media platforms.

[24] Katharine Silbaugh and Adi Caplan-Bricker, *Regulating Social Media through Family Law*, 15 U.C. Irvine L. Rev. 1 (2024).

[25] Brown v. Entertainment Merchants Ass'n, 564 U.S. 786 (2011).

[26] I made a similar argument regarding sexually explicit content in the pre-social media era. Ashutosh Bhagwat, *What If I Want My Kids to Watch Pornography?: Protecting Children from "Indecent" Speech*, 11 Wm. & Mary Bill of Rt.s J. 671 (2003).

[27] Meyer v. Nebraska, 262 U.S. 390 (1923) (striking down law prohibiting the teaching of modern languages other than English); Pierce v. Society of Sisters, 268 U.S. 510 (1925) (striking down law requiring students to attend public, not private, schools).

Family law is thus a striking instance of a long-standing body of law which can inform, and advance, legitimate restrictions on platforms. And because parental rights are so fundamental to our society (and have constitutional status), they do not always have to yield to the First Amendment. Rather, family law principles must be reconciled with legal protections, such as First Amendment rights, that platforms enjoy. Of course, this does not mean that parental wishes always should prevail. Family law itself requires that parents and guardians exercise their rights consistent with the basic well-being of children. So, for example, parents using their rights to harm LGBTQ minors by cutting off their access to online support communities would raise serious concerns. And I personally have doubts about the wisdom, and perhaps the constitutionality, of permitting parents to fully control social media access for older minors, say above the age of 16, who are on the verge of adulthood. But all that said, family law remains an important potential source of regulatory authority over platforms, in the same way that family law permits the state to empower parental control over other aspects of their children's upbringing.

There are thus many ways in which the application of existing law, or the creation of regulatory regimes built on existing legal regimes such as family law, can address some of the concerns raised by social media platforms without violating the principles of skepticism and presumption against new regulation that began this chapter. Unlike entirely new regulatory initiatives such as the EU's Digital Services Act (discussed extensively in Chapter 6), the application of general, established law to social media platforms does not rest on limited knowledge, nor is it vulnerable to changing technologies and business models. We have been enforcing contracts, imposing tort liability, and protecting parental authority for centuries if not millennia, and we have been enforcing antitrust law for well over a century. Applying such existing principles to platforms thus represents continuity, not legal experimentation.

8.3 SECTION 230 REFORM

Furthermore, while there should be a strong presumption against new laws specifically targeting social media platforms, that presumption is not absolute. There are certain forms of egregious harm associated with platforms, especially platforms that specialize in hosting harmful content, that are sufficiently pervasive, and that we are sufficiently familiar with, that it is probably time to address them. And, to address them effectively, it is probably time to consider amending, albeit in limited ways, that bastion of internet freedom, Section 230.

Recall from Chapter 6 that Section 230 has two primary provisions. The first, Section 230(c)(1), as interpreted by courts, shields platforms completely from liability for third-party content that they host. The second, Section 230(c)(2)(A), grants platforms the right to engage in good faith content moderation without risking liability. Between them, the two provisions of Section 230 effectively give platforms an almost free hand to host, or refuse to host, whatever content they choose. And while regularly criticized as a free pass, or a get-out-of-jail-free card, most commentators would acknowledge that Section 230 has enabled the creation and growth of the modern internet, including social media platforms.

But as law professor and MacArthur fellow Danielle Keats Citron points out, Section 230 has a dark side. Because Section 230 shields *all* platforms from liability, essentially without condition, it protects platforms who seek out, and specialize in hosting, deeply harmful content such as nonconsensual intimate images (including revenge porn), deepfake videos (often sexually explicit ones depicting actual individuals), and violent threats.[28] And while Section 230 of course does not protect the users who post such materials, they are often anonymous or difficult to locate, and so in practice unaccountable. Meanwhile, the owners of such platforms profit off the harm that their users impose on powerless victims. The problem, in simple terms, is that while Section 230 *permits* platforms to moderate harmful content, it does not require them to do so even if the content is defamatory or otherwise illegal (such as explicit deepfakes and threats).

It should be noted that Section 230 already acknowledges this problem, to some extent, and carves out some situations where immunity is not assured. In particular, from its origin, Section 230 exempted from its immunity shield any content in violation of federal criminal law, including obscenity and child pornography, and content in violation of intellectual property (IP) protections.[29] In addition, in 2018 in the "Allow States and Victims to Fight Online Sex Trafficking Act" (FOSTA) statute, Congress exempted from Section 230 immunity civil and state criminal laws relating to sex trafficking.[30] These exemptions, especially the IP one, make it clear that narrow Section 230 carve-outs, designed to address serous social problems, need not spell the death of the internet, contrary to some hyperbolic claims.

On the other hand, it must be conceded that actual experience with these carve-outs, especially the IP and FOSTA ones, has been mixed at best. With

[28] Danielle Keats Citron, *How to Fix Section 230*, 103 B.U. L. Rev. 713, 718 (2023).
[29] 47 U.S.C. § 230(e)(1) and (2).
[30] 47 U.S.C. § 230(e)(5); Citron, *supra* n. 28, at 722.

IP, the main (and highly predictable) problem that has emerged is excessive takedowns. The way in which the Section 230 IP exception and the 1998 Digital Millennium Copyright Act (DMCA) operate in tandem is that platforms receive notices from IP holders claiming that content that they are hosting violates IP law. If platforms then fail to take down infringing content, they face liability. In principle, of course, platforms could conduct an independent investigation to determine if the targeted content is in fact infringing (and leave up non-infringing content). But in practice their safest bet is to take down any content which might conceivably be found to violate IP rights. And that is exactly what we see happening, as the Electronic Frontier Foundation has documented.[31]

The story with FOSTA is more complex. As Professor Citron recounts, FOSTA was passed with the entirely admirable goal of helping victims of sex trafficking, by preventing platforms from enabling trafficking (and profiting from it). Unfortunately, that is not what has happened. Instead, concerns about liability under FOSTA incentivized platforms of all sorts to proactively ban any content even distantly related to sex work (note the parallel to IP), which has caused enormous harm to consensual sex workers by depriving them of safe places to connect to clients and to share information among themselves.[32] At the same time, FOSTA does not appear to have had any significant impact on the extent of actual sex trafficking, for complex reasons.[33]

The experience with FOSTA should give us pause in contemplating Section 230 reform. But Citron persuasively argues that many of FOSTA's problems are a product of vague language and bad drafting, which can be avoided if reform efforts are written carefully and narrowly.

As a starting point, under such a careful approach, there are simply no grounds for changing Section 230(c)(2)(A)'s protections for good faith content moderation by platforms.[34] There is no evidence that current content moderation practices are the source of systematic harm (despite the conservative claims discussed in Chapter 1), and in any event as Chapter 4 notes, in the *NetChoice* cases the Supreme Court correctly held that platforms have a First Amendment right to engage in content moderation.

Section 230(c)(1), however, is a different story. As Professor Citron recounts in detail, Section 230 has permitted bad actors to create literally thousands of websites (she counts 9,500 in 2020) dedicated to extremely harmful content, mainly nonconsensual intimate images. Indeed, Section 230 incentivizes

[31] Electronic Frontier Foundation, *Takedown Hall of Shame*, www.eff.org/takedowns.
[32] Citron, *supra* n. 28, at 738–40.
[33] *Ibid*. at 740–42.
[34] *Ibid*. at 746–50.

websites that are banned in other countries because of privacy violations to set up shop in the United States, where Section 230 and limited jurisdiction shield them from foreign enforcement efforts.[35] Citron's proposed solution is to enact a new and narrow exemption from Section 230(c)(1) immunity for platforms that "purposefully or deliberately solicit, encourage, or keep up material that they know or have reason to believe constitutes stalking, harassment, or intimate privacy violations," the latter term being defined as essentially nonconsensual nude or sexual images.[36] This proposal by and large fits the criteria of being extremely narrow, carefully defined, and limited to consciously bad actors.

The only part of this proposal that raises concerns for me is the phrase "reason to believe." It is included presumably because of the difficulty of proving that a platform knows that particular content falls within the carve-out. But because the resulting legal rule is somewhat amorphous (how much do you have to know, to have "reason to believe"?), it clearly incentivizes some prophylactic takedowns in response to insincere complaints – exactly the same problem associated with the IP and FOSTA Section 230 carve-outs. On the other hand, because the content covered by this proposed carve-out is so carefully and narrowly defined, as compared to the DMCA and FOSTA, a small amount of over-zealous content moderation may well be worth the price of protecting millions of innocent victims. At a minimum, Congress should give serious attention to such a proposal.

Citron's other proposal is to impose a "duty of care" on all platforms, which would condition Section 230(c)(1) immunity on platforms being able to demonstrate that they have taken "reasonable steps to address intimate privacy violations, cyber stalking, or cyber harassment,"[37] including creating mechanisms for victims to report such harmful content, and for platforms to investigate and ultimately take down offending material.[38] In the summer of 2024, US Representatives Jake Auchincloss (Democrat of Massachusetts) and Ashley Hinson (Republican of Iowa) jointly introduced legislation in Congress, the *Intimate Privacy Protection Act*, that would implement Citron's proposal, but adding, to the list of targeted content, pornographic deepfakes.[39] The benefit

[35] *Ibid*. at 728–30.
[36] *Ibid*. at 750–51.
[37] *Ibid*. at 753.
[38] *Ibid*. at 756.
[39] *Release: Auchincloss Introduces Bipartisan Bill to Tackle Rise in Non-Consensual Deepfakes on Social Media Platforms*, https://auchincloss.house.gov/media/press-releases/release-auchincloss-introduces-bipartisan-bill-to-tackle-rise-in-non-consensualdeepfakes-on-social-media-platforms.

of this approach is that it provides platforms who want to be good actors with a safe harbor – as long as they take reasonable and defined steps to identify and take down content invading intimate privacy, they will not be held liable for the occasional, and inevitable, mistakes. This can create a comfort level which reduces (though does not eliminate) the risk of excessive takedowns. And again, because the harmful content being targeted is carefully and narrowly defined, any harms associated with unnecessary takedowns would be very limited. Congress should give serious consideration to the Auchincloss/Hinson measure.

Professor Citron's article and the proposed legislation based on it address one set of very specific and serious issues: intimate privacy violations, stalking, and harassment. The sheer scale of this problem (which almost always victimizes women and girls) justifies legal reform, so long as it is undertaken carefully. It is tempting to move from this to propose a whole series of other carve-outs for other troubling content. But absent strong proof of a widespread and extremely serious problem, of the sort that Professor Citron and others have gathered,[40] I would resist that temptation.

It is important to remember that, for all of the reasons discussed in Chapter 6, Section 230 is very, very important. It enables platforms to operate and users to reach broad audiences. If we carve up Section 230 too much, converting it into Swiss cheese, at some point the effect will be the same as repealing Section 230 altogether. Imposing potential liability for a wide variety of user content will cause platforms to either simply abandon third-party content, or to engage in such aggressive content moderation as to silence enormous amounts of protected and harmless speech. In other words, weakening Section 230 too much will effectively end the *social* aspect of social media platforms, which is its capacity to permit millions, if not billions, of users to freely share content. And that would be a very unfortunate outcome.

8.4 PROCEDURAL RIGHTS FOR USERS

One important, difficult, and contentious question is whether regulators can and should grant users procedural rights vis-à-vis social media platforms. By procedural rights, I mean in general some sort of a legally enforceable right to notice from platforms, along with some explanation, when platforms take negative action against a user such as blocking or deemphasizing user content, as well as some right to internal review/appeal of the negative decision. On its

[40] Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1909–28 (2019); Mary Anne Franks, *"Revenge Porn" Reform: A View from the Front Lines*, 69 FLA. L. REV. 1251, 1261–77 (2017).

face, procedural rights seem fair and reasonable, given platform power over their users. But on closer examination, procedural rights raise extraordinarily complex issues.

The arguments in favor of procedural rights seem simple enough, and parallel the broader arguments in favor of due process in the judicial system. The first and most obvious is, of course, that process enhances accuracy. Requiring a statement of reasons guards against arbitrary or ill-considered actions, and internal review provides a check against platform errors in content moderation – something that even Mark Zuckerberg has conceded are extremely frequent.[41] Of course no level of process can assure that no errors occur; but the idea that procedural rights reduce the likelihood of error is the basis of our entire legal system (and in the Anglo-American tradition can be traced back to Magna Carta).

In addition to reducing error, procedural rights also advance some more fundamental, dignitary values. In particular, granting individuals procedural protections and the right to participate in decisions about themselves gives them a sense of being taken seriously, and treated fairly, quite independently of whether the process reaches the "right" result, or if the individual prevails.[42] These dignitary interests provide an independent reason, in addition to accuracy, to grant procedural rights to users, though in some sense both of these interests fall within the general rubric of "fairness."

Given the strong values advanced by procedure, one might think that giving users robust procedural protections is an obviously justified step. But there are important countervailing arguments. Indeed, at some point those arguments have constitutional dimensions because granting procedural rights to users can significantly burden platforms' own editorial rights. In Chapter 4 we saw that in the *NetChoice* cases, the Supreme Court recognized that platforms enjoyed a First Amendment right to control the content that they host or refuse to host, analogizing to cases that recognized such rights for earlier media including newspapers and cable television operators. But consider newspapers in this context. Imagine if a regulator or legislature required newspapers, when they decline to print a letter to the editor submitted by a reader, to provide the reader with a voluminous explanation for the rejection. As a practical matter, this would place an enormous burden on newspapers, and indeed would lead many of them to stop publishing letters from the public. For that reason, such a requirement would surely be found to violate newspapers' First Amendment editorial rights.

[41] *See supra* ch. 6, n. 52 and accompanying text.

[42] *See* Jerry Mashaw, *Administrative Due Process: The Quest for a Dignitary Theory*, 61 B.U. L. REV. 885 (1981).

Exactly the same argument can be extended to social media platforms. Indeed, because of the sheer scale at which platform content moderation occurs, providing detailed explanations for moderation decisions could potentially be sufficiently burdensome to effectively force platforms to eliminate content moderation. Facebook, for example, is reported to review three million flagged items of content on a daily basis.[43] And YouTube stated to the Fifth Circuit in the *NetChoice* litigation that it removed over a billion comments over a three-month period in 2020.[44] Newspaper editorial decisions are by comparison child's play. So even given the availability of automation to platforms, at some point the burden of explanation and review would become unsustainable.

Even aside from the burdensomeness of disclosure-and-review requirements, there is at least an argument to be made that requiring disclosure of the reasoning behind editorial decision-making is inherently unconstitutional. Indeed, with respect to newspapers and other traditional media, the argument is a powerful one. In a case arising out of a defamation claim against a magazine and a television broadcaster, the US Supreme Court stated that a "law that subjects the editorial process to private or official examination merely to satisfy curiosity or to serve some general end as the public interest … would not survive constitutional scrutiny as the First Amendment is presently construed."[45] Admittedly, the Court then went on to permit discovery into the editorial process as part of resolving a specific defamation claim; but the Court's broader language strongly suggests that an across-the-board requirement to explain editorial decisions, if addressed to traditional media, would be found unconstitutional.[46]

Whether to extend this logic to social media platforms, however, poses a difficult question. On the one hand, as the Supreme Court recognized in *NetChoice*, platforms enjoy the same sorts of editorial rights as traditional media, including presumably the right to make editorial choices for contradictory, no, or inconsistent reasons (the Eleventh Circuit suggested as much in its *NetChoice* decision[47]). But it must be acknowledged that social media

[43] John Koetsier, *Report: Facebook Makes 300,000 Content Moderation Mistakes Every Day*, Forbes (June 9, 2020), www.forbes.com/sites/johnkoetsier/2020/06/09/300000-facebook-content-moderation-mistakes-daily-report-says/.

[44] NetChoice, L.L.C. v. Paxton, 49 F.4th 439, 487 (5th Cir. 2022), *vacated and remanded* Moody v. NetChoice, LLC, 144 S. Ct. 2383 (2024).

[45] Hebert v. Lando, 441 U.S. 153, 174 (1979).

[46] The Fifth Circuit found otherwise in the *NetChoice* litigation, in the course of upholding a part of Texas's HB 20 which imposed an explanation-and-review requirement on platforms. *NetChoice v. Paxton*, 49 F.4th at 487–88. But the Fifth Circuit's reasoning in that case was so thoroughly debunked by the Supreme Court on appeal that it need not be taken seriously.

[47] NetChoice, LLC v. Attorney General, Florida, 34 F.4th 1196, 1222 (11th Cir. 2022), *vacated and remanded* Moody v. NetChoice, LLC, 144 S. Ct. 2383 (2024).

platforms are different from other, traditional media. Their almost complete reliance on third-party content itself distinguishes them from traditional media such as newspapers, magazines, and broadcasters (though not from cable television operators). And their relatively *laissez faire* attitude, permitting most content to go up while moderating a relatively small fraction, helps create an expectation on the part of users that they will be hosted, unlike with letters to newspaper editors. Furthermore, for many individuals and small businesses, access to social media plays a far more central role in their lives and livelihood than being published in a newspaper.

Another distinction between platforms and newspapers is that platforms *already* in most instances *voluntarily* provide some forms of explanation and review to users. Meta, for example, states that when it identifies content that violates Facebook Community Standards or Instagram Community Guidelines, "Meta will remove it. We'll also notify you so you can understand why we removed the content and how to avoid posting violating content in the future."[48] It also states that if content is removed, "we offer appeals for the vast majority of violation types on Facebook and Instagram."[49] And furthermore Meta, admittedly uniquely among platforms, offers the possibility of a further appeal of a unfavorable content decision to its Oversight Board.[50] Of course not all platforms provide as extensive user protections as Meta (and not all platforms engage in such extensive content moderation); but Meta's experience does suggest that granting users some procedural protections is consistent with robust content moderation.

All of these factors help to distinguish platforms from traditional media, and so cut in favor of recognizing *some* user rights with respect to platforms. On the other hand, the concerns about the burdensomeness of elaborate procedural obligations, and their likely negative impact on content moderation, cut in the opposite direction. How to balance these competing considerations is, quite frankly, a conundrum, and it turns significantly on very practical considerations about just how burdensome specific procedural rights would be – information that is only available to the platforms themselves (if even that). Furthermore, there is an argument to be made that business considerations alone (meaning retaining users) may well sufficiently incentivize platforms to protect users, so no state intervention is necessary. And there is also a very real

[48] Meta Transparency Center, *Taking Down Violating Content* (Feb. 22, 2023), https://transparency.meta.com/enforcement/taking-action/taking-down-violating-content/.

[49] Meta Transparency Center, *Appealed Content: What Can Be Appealed* (Nov. 18, 2022), https://transparency.meta.com/policies/improving/appealed-content-metric/.

[50] Meta Transparency Center, *How to Appeal to the Oversight Board* (April 3, 2024), https://transparency.meta.com/oversight/appealing-to-oversight-board/.

concern that when regulators *do* impose procedural obligations on platforms, as Texas did in HB 20, the true motivation may well be to hamstring platform moderation practices rather than to benefit users. These arguments raise serious doubts about the wisdom of any regulatory imposition of procedural obligations on platforms.

On balance, however, I am inclined to think that some regulatory intervention here may be justified and will not be unduly burdensome. Articles 20 and 21 of the EU's Digital Services Act (DSA), which as noted earlier was enacted in 2022 and is now in effect, grants precisely such rights to platform users, including a right to an internal appeal and a right to appeal further to an out-of-court dispute settlement entity designated by member nations.[51] This suggests that granting at least a right of internal appeal may well be a manageable burden, so long as elaborate explanations are not demanded of platforms. On the other hand, I do worry that the further right to external review, and potential judicial review, that the DSA envisions might impose very significant burdens, especially on smaller platforms, and so might be inadvisable (the EU is famously insensitive to such concerns, making it a rather poor role model for regulators). But I see no fundamental objection to a federal statute in the United States requiring platforms to create an internal review system for content moderation and deplatforming decisions, recognizing that some smaller platforms may be able to successfully challenge the application of such a law to them, on the grounds that it is excessively burdensome.

Procedural rights, in short, is another area where *some* regulatory initiatives may well be justified, simply in the name of fairness. But as always in this sensitive area, regulators must be sure to carefully thread the needle between protecting users and burdening platforms. And as always, courts must be available as a backstop to block excessively burdensome regulation.

8.5 DATA PRIVACY

The last area of possible regulatory reform that I will touch on is, unsurprisingly, data privacy. This is an area, as discussed in Chapter 7, in which there has been significant regulatory movement in recent years, including the EU's GDPR and California's Consumer Privacy Act (CCPA), as well as similar statutes in other states. In the United States, however, there has been no significant progress toward *national* privacy legislation, despite growing bipartisan

[51] *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)* Arts. 20 and 21, https://eur-lex.europa.eu/eli/reg/2022/2065/oj.

calls for such legislation and the obvious benefits (for both individuals and platforms) of a uniform nationwide regulatory regime. There is a strong argument that the time has come to close that regulatory gap. And it should be noted that any privacy legislation should be targeted not at social media platforms' data practices specifically but rather at all online data collection and processing.

The basic contours of needed federal privacy regulation seem relatively clear. First and foremost, it is entirely legitimate to require holders of personal data to take reasonable steps to prevent inadvertent disclosures and hacks. Given that the harms of data disclosures fall primarily on data subjects, but the power to prevent disclosures lies with data holders, the latter obviously have insufficient incentives to guard against inadvertent disclosures or hacks. The law can legitimately seek to correct this imbalance.

In addition, at a minimum, as with essentially all extant privacy laws, federal legislation must give the subjects of data collection some basic rights, including the right to be informed regarding how their data is collected, stored, and used; a right to access their personal data; and a right to have incorrect data be corrected. In addition, such legislation should probably include a right to object to the transfer or sale of especially sensitive data. These rights parallel the rights granted in the GDPR, CCPA, and other similar (sometimes copycat) state and national legislation around the world. And they are essential if data subjects are to be able to protect themselves from privacy violations and other misuse of sometimes highly personal information.

Why these rights are needed is straightforward. Basic notice about data practices are essential because otherwise users/data subjects have no ability to exercise their other data rights, or to choose to simply decline to use the relevant service, if the service providers' data practices seem too intrusive. The right to access personal data is similarly necessary to make other rights, including the right to correct inaccurate data, meaningful. Furthermore, being able to determine/confirm the content of the data collected by any particular entity also has obvious relevance in determining whether to consent to further transfer of the data. After all, my personal interest in keeping my work email and phone number (both freely available on the internet) private is far less pressing than it is, say, for medical or financial data, or even data regarding buying and web browsing habits.

Being able to correct inaccurate data is also fundamental to meaningful data privacy. While some data inaccuracies (say having a data subject's phone number wrong) can be fairly harmless, and indeed sometimes beneficial (fewer spam calls and texts), others can be effectively defamatory. Thus if a database inaccurately reports that one has filed for bankruptcy (as happened

in a leading US Supreme Court defamation case[52]), this can have serious economic and social repercussions. Similarly, albeit less seriously, inaccurate data about purchasing habits can result in being inundated with irritating and pointless advertising. Furthermore, it is hard to conceive of why a data holder would have any legitimate interest in maintaining inaccurate data. Of course, data correction rights do impose some costs on data holders; but the European and California experiences suggest that the costs are quite manageable (in part because such rights are rarely exercised, as discussed further later).

Finally, we come to what is potentially a more controversial right: the ability to opt out of data transfers and sales. This right implicates a more profound legal/ethical question, which is who "owns" personal data, the subject of the data or the data holder. The EU clearly views data subjects, if not as "owners" of data, as having fundamental rights to exercise control over their data – that is indeed what the first two findings in the preface to the official text of the GDPR, as well as Art. 1 of the GDPR, state.[53]

But at least in the US legal tradition, the truth of this proposition is not evident. After all, personal data that data holders collect was generally freely shared by data subjects, usually in exchange for valuable services (including such things as discounts at grocery stores[54]). And personal data is notoriously an article of commerce – reports suggest that the global data brokerage market will be worth close to $400 billion in 2024.[55] Normally in the US legal system we assume that when a valuable commodity (which data is) is exchanged for services, title to the commodity moves to the recipient. And unlike in the European tradition, US law is much more resistant to amorphous rights of personality which limit traditional property rights.

The preceding discussion would suggest that a right to object to data transfers and sales is in tension with existing property and contract law principles. But there are countervailing considerations. Most obviously, there are some specific types of highly personal data, such as financial and medical information, that even in the United States are already heavily regulated, because of the obvious harms associated with disclosure. That seems entirely appropriate, for the same reasons that we regulate the sale and distribution of other

[52] Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749 (1985).

[53] GDPR, *supra* n. 14, Findings (1) and (2), Art. 1.

[54] Devan Burris, *How Grocery Stores Are Becoming Data Brokers*, CNBC (Dec. 10, 2023), www.cnbc.com/2023/12/10/how-grocery-stores-are-becoming-data-brokers.html.

[55] Knowledge Sourcing Intelligence, *Global Data Broker Market Size, Share, Opportunities, and Trends by Data Type (Consumer Data, Business Data), by End-User (BFSI, Retail, Automotive, Construction, Others) and by Geography – Forecasts from 2025 to 2030* (Dec. 2024), www.knowledge-sourcing.com/report/global-data-broker-market.

harmful items. And with respect to such highly sensitive data, data holders are surely on implicit notice (and if and when legislation is enacted, explicit notice) when they collect and store the data that their ability to use or transfer that data is likely to be restricted.

All of this raises some doubts about the flat right granted by GDPR and CCPA to data subjects to completely opt out of data sharing and sales.[56] Such an unrestricted right enacts an across-the-board preference for data subjects over the arguably legitimate interests of data holders. But if data subjects (in the case of platforms, users) have obtained valuable benefits in exchange for sharing their data, it is not clear why such a flat preference is justified. Admittedly, there is an argument to be made that, when users share data, they do so knowing that the data will be used for commercial purposes (primarily to sell targeted advertising) but do not necessarily consent to the transfer or sale of non-anonymized data. So the question is a close one. My own inclination would be to limit the right to opt out of data sharing and sales to particularly sensitive data, as the CCPA does with respect to data use;[57] but certainly other reasonable people might support the kind of flat opt-out right that the EU and California currently grant.

In short, there is plenty of room for legitimate data privacy regulations, and a pressing need for national data privacy legislation in the United States. But that said, there are also important limits on what data privacy laws should seek to accomplish. Consider opt-out rights. There are, as just acknowledged, legitimate arguments in favor of the EU's and CCPA's grants of rights to opt out of data sharing and sales. But the GDPR goes beyond permitting an opt-out from data transfers. In addition, the GDPR expressly grants data subjects the right to stop processing for the purposes of direct marketing unless they have explicitly consented to such processing[58] – and the GDPR also grants the right to withdraw consent "at any time."[59] But there is obvious tension between these rights and the original bargain under which the data subject shared their personal information, knowing that it would be processed in exchange for specific services. Essentially, an unlimited opt-out right grants users a free lunch. Certainly, users have a right to insist that processing is limited to the uses that the user/data subject originally consented to. But the right to opt out of a bargain after having received (and presumably continuing to receive, in many instances) the benefits that were bargained for is an odd form of "fairness."

[56] GDPR, *supra* n. 14, Art. 7; Cal. Civ. Code § 1798.120.
[57] Cal. Civ. Code § 1798.121.
[58] GDPR, *supra* n. 14, Art. 21(2) and (3).
[59] GDPR, *supra* n. 14, Art. 7(3).

Similar objections can also be raised to the rights to data deletion/erasure, also granted by both the GDPR and CCPA.[60] But in addition to benefit-of-the-bargain arguments, this so-called right to be forgotten also threatens basic principles of free expression. Data is information, and information undergirds public discourse. And while much personal data has little relevance to public discourse, that may not be true regarding personal information about prominent individuals, especially historical information such as past criminal convictions or other misconduct. Most obviously, such information is highly relevant to judge the fitness for office of high elected and appointed government officials. For that reason, any right to data deletion should be phrased carefully and narrowly, to ensure that data subject to deletion is not of the sort that could have relevance to current or future public discourse. Neither the GDPR nor the CCPA have any such limitations.

Admittedly, both of those regulations qualify the right of data deletion, saying that it does not apply insofar as the data is necessary, in the GDPR's words, "for exercising the right of freedom of expression and information."[61] But it is hard to know what this vacuous qualification means, especially given that in many European legal systems privacy rights, even for prominent individuals, are regularly found to trump free speech rights. Moreover, it is hard to know in advance what information *will* be relevant to public discourse. For example, one could easily imagine an individual contemplating running for local elective office arranging to have negative information about themselves deleted prior to announcing the run, thereby shielding themselves from legitimate scrutiny. Data deletion is thus an area where regulators need to tread extremely carefully – which to date they have not done.

Underlying all of these concerns about the reach of data privacy laws is a broader point: There is a fundamental tension between data privacy and the business models of the major platforms (as well as related services such as search). That business model is based on an exchange of personal data for free services – services, it should be noted, that no one is obliged to use. Data privacy advocates sometimes seem to believe that this business model is illegitimate and should be abandoned. But then they bear the burden, which they have not even attempted to meet, of coming up with an alternative model for the provision of services such as social media and search. Absent a pay-for-use model, which it is hard to believe most users would prefer, the vision seems to be that rich Big Tech giants will simply hand these services out for free,

[60] GDPR, *supra* n. 14, Art. 17; Cal. Civ. Code § 1798.105.

[61] GDPR, *supra* n. 14, Art. 17(3)(a). The CCPA similarly exempts data necessary to "Exercise free speech." Cal. Civ. Code § 1798.105(d)(4).

indefinitely. But that is a fantasy. Someone has to pay the substantial costs of providing online services, and in the long term if the advertising-based model is undermined by law, that someone is going to be users.

One final caveat is necessary here regarding data privacy regulation: efficacy. Data privacy statutes such as the GDPR and CCPA grant data subjects broad rights to control their data, including accessing their personal data, deleting data, and opting out of the sharing and sale of data. But most of those protections are effective only if data subjects affirmatively assert their rights (the major exception is the GDPR's restrictions on data processing, which are in the main self-executing). So, do data subjects assert their rights? Because if they do not, privacy laws (at least in their current incarnation) are not doing much good. And on that point, a recent study's results are not encouraging.

The study was conducted by Ella Corren, then a doctoral candidate at the University of California, Berkeley School of Law. Corren took advantage of the fact that regulations issued by the California Attorney General in 2020 to implement the CCPA require large firms (defined as those that process the data of more than 10 million consumers in California a year) to file reports laying out how many data control requests they received, and how they acted on those requests.[62] Corren used these filings to compile a database of data control requests received by 137 firms in the year 2020, and 121 firms in 2021.[63] The database focuses on three data control rights: the right to know (meaning to access one's personal information), the right to delete such personal information, and the right to opt out of the transfer or sale of personal data.[64]

The results are somewhat stunning. In 2020 the vast majority of firms – 75 percent – reported fewer than 10,000 requests annually invoking *any* of these rights, which translates to fewer than 0.1 percent of these firms' data subjects. Indeed, the majority of firms report fewer than 1,000 requests, and 88 percent of firms report less than 100,000 requests, translating to at most 1 percent of data subjects. The number of requests in 2021 was slightly higher, but even in that year 73 percent of firms reported fewer than 10,000 requests for the most-invoked right (and 89 percent of firms reported fewer than 100,000 requests).[65] In short, what Corren learned was that for the vast majority (90 percent) of firms, 99 percent of their data subjects make no data requests; that for three-quarters of firms 99.9 percent of their data subjects make no requests; and for a solid majority of firms almost no data subjects make requests.

[62] Ella Corren, *Gaining or Losing Control? An Empirical Study of the Real Use of Data Control Rights and Policy Implications*, 109 Iowa L. Rev. 2017, 2023 (2024).
[63] *Ibid*. at 2033.
[64] *Ibid*. at 2023.
[65] *Ibid*. at 2035–36.

Digging slightly deeper into the data, one finds that the most-invoked of the three rights Corren included in her study is the right to opt out of data sales, by a small but significant margin. This is unsurprising because the right to opt out is the only one firms are required to highlight on their website, via a prominent "Do Not Sell My Personal Information" link.[66] In addition, it makes intuitive sense that this is the right that data subjects would care most about, because having one's data proliferate on the internet is obviously more threatening to privacy than having a single firm hold personal data. It should be noted, however, that for the major social media platforms this is also the least relevant right because, as noted in Chapter 3, they do not sell their users' data.

What are we to make of these findings, and what implications do they have for privacy regulation? It might be that regulators need to ensure that data holders provide consumers with prominent notice of all of their data control rights, including easy mechanisms for invoking them, as is true with opt-out rights. But it should be noted that even with respect to opt-out rights, 88–89 percent of firms report receiving fewer than 100,000 annual requests, meaning that fewer than 1 percent of their users invoke them. So while prominent notice might contribute to *some* greater uptake of data control rights, the impact appears to be small.

In truth, then, the main lesson of this study *might* be that people simply do not care all that much about data privacy. Admittedly, that is not what people say, but it does appear to be their revealed preference. If this is true (a contentious question), that cuts strongly against regulations which would undermine targeted advertising-driven business models for platforms, because the impact of such government action would be to take away from users something they care about (free services) in exchange for providing them something they do not much care about (data privacy).

The other possible lesson, however, is that while users might well care about data privacy, they do not want to bear the burden of protecting their own privacy. People are busy, life is hectic, and the instinct of even users who do value data privacy is to quickly click through consent buttons. Indeed, many prominent privacy scholars have made precisely this point, arguing that data control/consent laws are not a particularly effective way to protect data privacy.[67] Exploring that voluminous literature on how more effective privacy regulations might work is beyond the scope of this chapter and book. But one

[66] *Ibid*. at 2043–45.

[67] *See*, e.g., Daniel J. Solove, *The Limitations of Privacy Rights*, 98 Notre Dame L. Rev. 975 (2023); Ari Ezra Waldman, *Privacy's Rights Trap*, 117 Nw. U. L. Rev. Online 88 (2022); Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 Md. L. Rev. 952 (2017).

clear and striking lesson to take from all of this is that data control regimes, which are by far the most popular forms of data privacy regulation across the globe, appear to be quite ineffective, which raises serious questions about whether they are worth the costs of enactment, compliance, and enforcement.

* * * * * *

There is, in short, plenty of room for careful, targeted new regulation of social media platforms to address specific, empirically confirmed social issues. In this chapter, I have sought to highlight some possible regulatory initiatives that seem currently justified, without purporting to address the entire universe of possible government actions. But, it should be emphasized, even when action does seem necessary, an attitude of caution and skepticism regarding how to proceed remains in order, given how young social media platforms are and how quickly they continue to evolve.