MLRC Media Law Resource Center
BULLETIN

2021 Issue No. 1 June 2021

LEGAL FRONTIERS IN DIGITAL MEDIA

The Oversight Board at 6 Months: Will Facebook Rue the Day? • 3
Ross Ufberg

Going Big, One Problem at a Time: Europe's Regulation of Digital Services and Markets Gathers Pace • 11
Remy Chavannes, Anke Strijbos and Dorien Verhulst

Social Media Blocking by Government Officials – Where Does the Law Stand? • 27
Lyndsey Wajert

Managing Compliance with the Growing Patchwork of State Privacy Laws • 39
Phil Yannella, Kim Phan and Greg Szewczyk

Die Hard: Will Constitutional Roadblocks and a Lack of Consensus Stall Section 230 Reform? • 55
Ambika Kumar, Robert Miller, and Sarah Burns

The Oversight Board at 6 Months: Will Facebook Rue the Day?

By Ross Ufberg[1]

In January of this year, the Oversight Board (OB) created by Facebook issued its first set of decisions. It was a modest start: six cases deciding the fates of posts touching a wide swath of the world, from Azerbaijan and Armenia to Malaysia, Myanmar, France, and more. Since then, more decisions have trickled out, bringing the total to about a dozen, including the one regarding former President Donald Trump's indefinite suspension from Facebook immediately following the January 6 attack on the Capitol. The OB upheld Facebook's decision to suspend the former president, but kicked it back to the platform to set a time limit on the suspension.

To rewind a bit: What is the Oversight Board? First, let's start with what it is *not.* It's not the Supreme Court of Facebook. It's not a court of law, period. It's not a governmental regulatory agency. It's not even part of, or owned by, Facebook. And it's certainly not a panacea to all of the ills of social media or an answer to all of life's most perplexing content moderation quandaries.

What it is, is an experiment.

Facebook, which has nearly three billion users, has bandied about the idea of a Sanhedrin to preside over its content moderation policies and decisions for a few years now. On a podcast in 2018, Facebook CEO Mark Zuckerberg spoke of "some sort of structure, almost like a Supreme Court, that is made up of independent folks who don't work for Facebook, who ultimately make the final judgment call on what should be acceptable speech in a community that reflects the social norms and values of people all around the world." That's a tall order: finding, and then reflecting, consensus on the social norms and values of around three billion people.

In a typically Facebookian way—elaborate, data-rich, overblown—the composition and mechanisms of the OB have been workshopped and round-tabled 28 times with 650 people, in 88 countries, the results were written up in a 224-page report, and Facebook had personal discussions with 250 people, and received written feedback from 1,200 more.

With this origin story, the OB was sent out into the world in 2019, with $130 million in funding from Facebook to get rolling. That's not peanuts, but for a company that took in over 84 billion dollars in ad sales last year, that allocation represents about .15% of their annual revenues.

Eventually, the OB hopes to have forty board members. Right now, they're hovering around 20. In a sign of either assertive independence or extreme self-importance (or both), the body is officially called The Oversight Board LLC. Not, as one might expect, the Facebook Oversight Board. It is an entity separate from Facebook, created by and for it, but living a life distinct from

[1] Ross Ufberg is a rising 3L at Berkeley Law School. He's currently a summer associate at Dechert LLP in Philadelphia. In a previous life, Ufberg was a journalist, and founded the publishing house New Vessel Press.

it. Think of it as Frankenstein's creature, but before the creature has actually gone and strangled anybody.

The OB is staffed with law professors, human rights and free speech advocates, experts in digital and constitutional rights, and in governance. The tilt is noticeably international. Board members hail from around seventeen different countries; the U.S. is the most represented country, with five members.

The board's purpose, as per its Charter, "is to protect free expression by making principled, independent decisions about important pieces of content and by issuing policy advisory opinions on Facebook's content policies." Its goal is not to make three billion people happy. "That would be an utterly impossible task," admitted Director of the Oversight Board Thomas Hughes, while participating on a panel at the MLRC's Legal Frontiers in Digital Media Conference 2021.

The board will be guided by international human rights principles, and Facebook, as per the Bylaws of the Oversight Board, "will respond to all board decisions publicly through its newsroom. It will provide a statement documenting its implementation of each of the board's content decisions."

Here's a brief explanation of the nuts and bolts of how it works.

When a Facebook user has content taken down, they can appeal that decision to Facebook. Facebook removes billions of pieces of content each year. Users appeal only a tiny percentage of those takedowns. Facebook may decide to reinstate a contested takedown; they may decide to stick to their guns. At that point, once all the internal options have been exhausted, the user may file an appeal to the Oversight Board, through a link on the board's website. But the odds are against the user: the OB will most likely *not* take any given appeal, since at full throttle it'll consist of forty members, most (all?) of whom have other jobs. As of now, there have been about 300,000 appeals to the OB; the board has taken about a dozen of them.

Another criticism of the august board has to do with the elevated status and high finances of a body that will make a few dozen, a few hundred, at most, content moderation decisions per year. Any foot soldier doing low-level content moderation for Facebook must make several hundred decisions per *day*. The OB's cases will just be a drop in the content ocean.

Still, if they do take a case, a five-member panel of the board will deliberate on it and issue a ruling. If they decide that Facebook was wrong in taking down a piece of content, they can order Facebook to put that post back up. But here's the rub. While their decision is binding on Facebook, it is only binding as to that single piece of content. Even an identical post will not necessary be reinstated, or deleted—Facebook will consider the context of each post in making its decision.

Let's take an example. Say a user posts a quote attributed to Nazi Propaganda Minister Joseph Goebbels. The quote encourages arguments that appeal to emotions, discourages arguments that are overly intellectual, and claims that the truth doesn't matter, and anyway, it's the people on the street with muscle and brawn who will win the day.

Facebook then takes down the post as violating the Community Standard on Dangerous Individuals and Organizations. The user disagrees, exhausts his remedies within Facebook itself, and appeals to the Oversight Board. Against all odds, the board accepts the case, and during its investigation discovers that, actually, the post was meant to draw a comparison between Goebbels—somebody the user felt was an evil figure from the past—and a current political leader. At its core, the post—which was satirical—did quite the *opposite* of supporting a dangerous individual's speech. (And as the OB pointed out in a different case, Facebook does in fact have a satire exception, it's just not public.) The post was trying to raise awareness of the dangers of certain types of rhetoric today, by tying it to dangerous rhetoric of the past. Recognizing this, the board orders Facebook to restore the post, and also issues a few nonbinding policy recommendations, including that Facebook publish a list of the organizations and individuals designated "dangerous" under the Dangerous Individuals and Organizations Community Standard.

That's a good outcome, right? In a very narrow sense, yes. But Facebook is only bound to reinstate that single post. It is not obligated to restore identical posts by different users. And it can feel free to disregard the policy recommendations; those are never binding. (If you're wondering, those details are from a real case, by the way: Case Decision 2020-005-FB-UA.)

David Post, a retired law professor and adjunct fellow at the Cato Institute, has leveled similar criticism at the actual reach of the board's powers. "Facebook will take 20 or 30 *billion* enforcement actions in 2021," Post wrote on the Volokh Conspiracy blog. "The Board has the power – but *only* the power – to decide what happens in an infinitesimal handful of them (50? 100? 200?). With respect to everything else happening in this immense ocean of content, *Facebook can continue to do whatever it wants to do regardless of what Board decides.*"

Another skepticism has to do with the enforcement of its powers. What happens if the board issues a ruling Facebook really doesn't like? In Federalist 78, Alexander Hamilton wrote of the judiciary, "It may truly be said to have neither FORCE nor WILL, but merely judgment; and must ultimately depend upon the aid of the executive arm even for the efficacy of its judgments." If the Oversight Board, with "no influence over either the sword or the purse" of Facebook, is completely dependent upon the continued willingness of the company to comply with its decisions, how much power is that really?

One answer—Pollyannaish, but also maybe true? — is that whatever power the OB has, it's more power than any other independent actor had over the company before. And the soft power of the board, outside of whether an individual piece of content gets restored to the site, may turn out to be considerable—its best, its only, true weapon. Repeated call-outs in OB decisions or by board members in the public square have the potential to make Facebook extremely uncomfortable. What if board members grow resentful from seeing their decisions and recommendations not being implemented, or not being implemented in the manner and with the breadth they desire? Might they campaign publicly against Facebook? Might Facebook have created and funded its own most vocal, most prominent adversary?

But the most important limit on the OB's power doesn't have to do with the reach of their decisions, but with the jurisdiction that defines their reach.

And that's the question of the algorithm. "Facebook very clearly said from the outset that the algorithm, the coding, as it were, was not in scope of the board," said Hughes, the board's director. While I am scrupulously avoiding the ins and outs of the Trump decision—much ink has been spilled already—there's one point, perhaps the only point of that whole decision, actually, that really matters.

Facebook is not merely a giant thumbtack board where individuals post their pictures, share their stories, and sell their products. It's a board with a brain—which sees which stories get read, which photos get viewed, which posts get clicked, and then does some magic and decides what will go viral, what will die a death unnoticed. Nobody outside of Facebook knows exactly how they make those decisions. Nobody knows why the computer brain—programed by people, presumably with human brains—chooses to promote, progress, prevent, process, protect, in the way it does. That's broadly speaking the algorithm of Facebook. That's the secret sauce, what makes it addicting, clairvoyant, irresistible. That's what makes Facebook incredibly powerful.

During the course of their deliberations, the board asked Facebook for more information about how the platform's own actions may have contributed to the reach and effect of Trump's posts.

> "The Board sought clarification from Facebook about the extent to which the platform's design decisions, including algorithms, policies, procedures and technical features, amplified Mr. Trump's posts after the election and whether Facebook had conducted any internal analysis of whether such design decisions may have contributed to the events of January 6. **Facebook declined to answer these questions.** This makes it difficult for the Board to assess whether less severe measures, taken earlier, may have been sufficient to protect the rights of others." Trump Decision p.29

This is perhaps the most consequential paragraph in any of the board's rulings yet. An admission, a nod, to the limits of power, begging the question: without knowing how the system works, how can you police the system?

The system—Facebook—is an incredibly potent weapon to be wielded. More potent, perhaps, than any "soft" weapon the world has ever seen before. Social media has opened up more avenues for speech, more avenues for grievous wounds.

Of course, this would not be news to the folks on the OB. Suzanne Nossel is the board's newest member. Nossel is also the Chief Executive Officer of PEN America, whose mission "is to unite writers and their allies to celebrate creative expression and defend the liberties that make it possible." She is a strong and prominent advocate of free speech. At PEN, she told me, "We have frequently sounded alarm bells about the unfettered discretion that social media platforms and other private companies hold over public discourse, urging transparency and accountability, and pressing the companies to establish clearer guidelines—rooted in international human rights law—to govern the moderation of online speech." As a board member, that'll pretty much be her job description.

Nossel calls this an "experiment," one she's entering into with "open eyes." She pointed me to a report issued by her organization—a report she helped edit—which noted, "There is also a growing recognition that the design of these platforms—from user experience and product features to the underlying algorithms—are inextricable from the targeted advertising and attention economy that underpins their business models."

For Santa Clara law school professor Eric Goldman, a prominent commentator on technology law, Facebook's refusal to share its algorithm doesn't necessarily mean its designs are evil. It's just that the company's objectives and the Oversight Board's objectives aren't necessarily coextensive. The OB has a narrow purview: to make decisions based on international human rights considerations. Yet, Facebook cannot possibly make decisions based on those criteria alone. It's a for-profit company which has all the prerogatives a for-profit, public company usually has. "Facebook has a number of good reasons why it doesn't want more details publicly available about its algorithm," Goldman told me. "I'm sympathetic to the fact that Facebook isn't always going to do what the Oversight Board asks, because the Oversight Board is prioritizing only some of the considerations that fb has to balance."

Again, one answer may be that this at the very least shows us in clear outlines the limits of what Facebook is willing to do to moderate its content. It helps define the contours of the problem. If we learn more about what FB considers its secret sauce, by accretion of these decisions, then presumably a regulatory agency will know exactly where to poke the bear, to find where he's hiding the honey.

Something that the decisions have shown us, for sure, is just how difficult it is to imagine, and then define, a community of three billion users. Is that a community in any meaningful sense of the word, or is it just a very large number of people using a particular product? Are the three billion Facebook users a "community" any more than people who grew up eating with chopsticks are a "community," or people who drive in a car at least once a week are a "community"?

One case in particular crystalizes this difficulty. Oversight Board Case Number 2021-002-FB-UA revolves around a Dutch holiday tradition, virtually unknown in the United States, probably unknown to most of the Oversight Board members, yet widespread in the Netherlands. Zwarte Piet, or Black Pete, is a sort of Santa's assistant in the Netherlands' tradition. Zwarte Piet is, depending on the source, a blackface figure, or covered in soot from crawling down chimneys, apparently of Moorish origin.

Facebook's Hate Speech Community Standard prohibits "caricatures of Black people in the form of blackface." Last year, a few weeks before Christmas, a user in the Netherlands posted a video depicting a child greeting the Dutch Santa Claus along with not one, but *two* Zwarte Piets. One of the Piets puts a cap on the child's head as festive music plays.

Nobody on the board—neither those five members who partook in this particular case, nor any of the board in general—is Dutch; yet the OB, guided by international human rights standards, upheld Facebook's takedown of the post. Perhaps they sought "context briefs"—this is a thing they can do, according to Hughes—which is "an analysis of the local, or national, or regional, context in which the case is taking place," before making their decision.

The Zwarte Piet case attracted a paltry number of comments—twenty-two, compared to about 10,000 in the Trump case—a few of which came from the United States. One of those Americans who commented is Daniel Gainor, a right-wing media commentator who is a VP at Media Research Center, a non-profit dedicated to exposing alleged liberal media bias.

"If Facebook is going to start removing things in one culture that might offend members of another culture, it should just shut down right now," Gainor wrote. "This is such a stupid debate. There is no right to not be offended. And if that's the world Facebook's Oversight Board wants to create, then it will be seen as ridiculous as the original removal."

Just a few pages away, a neighboring comment from Lori Selke, a poet and author who publishes in the genres of dyke and experimental erotica, expressed a starkly different point of view. "Cultural nostalgia for colonialism and racism is not an excuse for posting content like this, and that's all that Zwarte Piet is, no matter how well-loved or fiercely defended. The U.S. fought an entire war to defend slavery, after all. The removal of the content should be upheld."

As somebody who can't fathom ever submitting a comment to the Oversight Board, I reached out to both of these Americans, to better understand their motivation for chiming in to an international, Dutch-free, board of content umpires, about to pass judgment on a Netherlands holiday tradition.

Gainor's answer was simple. Facebook is an American company. It ought to honor, if not be governed by, our country's most important constitutional principles. "The concept, the principles, of free speech, of the First Amendment, have insinuated themselves into our country. Much more in our country than in anywhere else in the world. To have a board that doesn't believe in those principles is disturbing," he told me. Yes, Facebook as a private company is free to be guided by international human rights standards rather than American free speech standards, but that, for Gainor, is beside the point. He hopes the comments influence the OB to guide Facebook closer to his jurisprudence. "If you don't demand the best of the most powerful company in human history, then you're going to get the worst."

On the other hand, Selke wrote to me, the First Amendment "does not apply (for better or for worse) to platforms like Facebook, which can moderate their content in any way they see fit." And how Facebook sees fit, she said, has been quite wrong: no "clear, identifiable standards" to what it permits, "no understanding of systemic inequalities," "a reliance on bots/or poorly trained workers" to monitor content. And so, while she would like for Facebook to fix those things, what she wants of the Oversight Board is for it to "incorporate an understanding of the historical and contemporary impact of colonialism, imperialism, and structural racism on what constitutes acceptable public discourse on the site. I know I might as well wish for the moon, but there it is."

Gainor would prefer a Facebook that is First Amendment absolutist; Selke told me, "I want it to be a humanizing platform."

What kind of single standard can possibly govern two viewpoints as far apart as that? Those are the views of two well-educated Americans, professional people of words, each with a sophisticated understanding of human rights and the First Amendment, each versant in the language of the American Constitution. What happens when you expand out—not just to Dutch

holiday traditions, but to Afghan wedding rituals, Chinese government propaganda posters, statements of support for anti-Muslim anger in France and videos stoking anti-French anger amongst Muslims, footage of Zionist and anti-Zionist protests and gatherings and clashes and on and on, toward infinity. What happens when your "community" is the world, and the content of the "content" is everything that goes on inside it?

* * *

Who can read the mind of Mark Zuckerberg? Maybe all of the foregoing is just a distraction. Maybe the Oversight Board is just a ploy to stave off regulators for an extra year or two, so they can see how this thing plays out. An attempt to get one or two more regulation-free years on the books. That's a cynical take, though not an entirely outlandish one: Facebook would likely do much better than simply make up its costs in financing the Oversight Board. The company's net income last year was $29 billion. The board cost them $130 million.

Whatever the Oversight Board is, it is off to the races, the cat is out of the bag, Frankenstein's creature is on the prowl and who knows if it will end up being the conscience or the cat's paw, the nag, the nudge, or of no consequence. And it is an experiment, an exciting one, even, staffed with scholars and activists who no doubt want to find the best balance between free expression and human rights.

"Some experiments don't work," Goldman told me. "And if this experiment works, it might not work for anyone other than Facebook." We should, like scientists in a lab, keep our eyes on the results: "What problem does the Oversight Board solve, what does it create, and does it solve more than it creates?"

The Oversight Board is like Damocles, working just beneath the double-edged sword of free expression on one side, and other human rights prerogatives on the other. It's not an easy or enviable task. They must figure out a way to keep the sword, dangling on a string, from swinging too far in either direction, or from dropping onto their heads.

Going Big, One Problem at a Time: Europe's Regulation of Digital Services and Markets Gathers Pace

Remy Chavannes, Anke Strijbos and Dorien Verhulst[1]

While European courts are still working to interpret digital laws from the early years of the century, the EU legislative machine is rapidly churning out new regulations and directives designed to protect online consumers and competitors from the perceived abuses and vast carelessness of the global tech platforms. The dominant narrative is that, after two decades of under-regulation benefiting mainly non-European companies, it is time for regulatory catch-up, with rules which are much more closely targeted at the digital services and problems of today. In the process, the contours of a European "law of the internet"[2] *are fast coming into focus. Coupled with major new initiatives in the sphere of data, data governance and artificial intelligence, all signs point to the emergence of an overarching EU regime for tech regulation – albeit one still struggling for coherence and consistency.*

Introduction

Comparing the paragraph above to our EU platform regulation update in this Bulletin from two years ago,[3] the reader may be forgiven for concluding that not much has happened in this area, or at least that the authors have failed to notice. After all, in 2019 we were already in the midst of the techlash, and Europe was already engaged in a process of tech re-regulation characterized by grand ambitions, a conviction that "these platforms" should be doing both "more" and "less", and a reluctance to make hard policy choices. Then, too, Brussels was preaching rules for artificial intelligence that would fully and equally protect all economic, social and moral imperatives. While it is true that we are still in the same process of burgeoning European assertiveness in digital regulation, the legislative proposals are becoming more far-reaching and more fundamental, driven by a broad political consensus that major steps are needed to bring online platforms and algorithms to heel. In times of pandemic, online services have proven their immense worth, but also increased concerns about their indispensability.

All the same, we should not exaggerate the speed of travel. The new EU rules which we discussed in 2019, regulating upload platforms, press publisher's rights, video-sharing platforms and online intermediation services, have barely entered into force at the level of individual EU member states. The European Commission's ambitious new proposals on digital services, digital

[1] The authors are attorneys at the technology and communications law firm Brinkhof in Amsterdam, where they specialize in copyright, media, and internet litigation. They would like to thank their colleagues Ella Meijaard, Sophie ten Bosch, Hanneke Kooijman, Leonie van Sloten and Bart Tromp for their valuable contributions. This update covers the period March 2019 - March 2021.

[2] A recent addition to the academic discourse on the existence and scope of such a thing as "internet law" is R. Leenes, 'Of Horses and Other Animals of Cyberspace' *Technology and Regulation*, 2019 pp. 1-9, retrieved from https://techreg.org/index.php/techreg/article/view/3.

[3] Remy Chavannes & Dorien Verhulst, 'Regulation of Online Platforms in the European Union – The State of Play', *MLRC Bulletin: Legal Frontiers in Digital Media* 2019 No. 1, pp. 3-15, retrieved from https://blog.chavannes.net/2019/05/regulation-of-online-platforms-in-the-european-union-the-state-of-play/.

markets, data and AI may not come into force before the MLRC's *Legal Frontiers in Digital Media* conference of 2023.

In recent years, the European tech debate has broadened and deepened, but also has become fiercer and more political. In the cacophony of hot takes, avidly shared in meme form on those same online platforms, opportunism and self-interest are more in evidence than informed debate or consistent policy. When online platforms, after years of being described as unchecked echo chambers of hate and disinformation, finally moved to ban President Trump and other policy violators following the Capitol riots, European politicians were quick to lambast them as arbitrary enemies of free speech in urgent need of regulation. Journalists at traditional European media outlets have increasingly followed their publishers in blaming online platforms for their own commercial troubles, with "paying for news" as the new "value gap" frame. Meanwhile, tech companies have preached "better regulation" while advocating rules that protect their own interests. While the debate over artificial intelligence is still relatively technical and niche, there is a growing awareness that algorithms can inherit the biases of their creators, users and the training data on which they have been raised.

Regulation of online intermediaries: the emerging EU law of the internet

The mostly quite targeted EU laws that made it over the legislative finish line just before the 2019 European Parliament elections are beginning to come into effect at the national level, affecting for example the transparency obligations of online intermediation services,[4] youth-protection obligations of video-sharing platform services[5] and copyright liability of upload platforms.[6] The newly installed European Commission and European Parliament are now working on much more ambitious projects, including rewriting the basic rulebook for digital services set out in the E-Commerce Directive from 2000,[7] and creating a new system of preventive competition oversight of digital markets designed to curb the power of the largest "gatekeeper" platforms.[8] These new proposals are predicated on the assumption that the large online platforms are doing both "too little" and "too much", and the fact that they can decide for themselves what, if anything, they do shows that they have too much power.

[4] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, applicable from 12 July 2020.

[5] Directive 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities.

[6] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

[7] The so-called Digital Services Act (DSA): Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825 final dated December 15, 2020.

[8] The so-called Digital Markets Act (DMA): Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act), COM(2020) 842 final dated December 15, 2020.

Combating illegal and undesirable content

Of all EU citizens, 65% use at least one social media service every day.[9] According to a growing number of critics, the way in which a handful of California-based tech companies are managing these services is too opaque and too arbitrary. The call for greater transparency and accountability is particularly strong with respect to content moderation: the formulation and enforcement of rules by online platforms determining what can and cannot be said on their services. This is hardly surprising: take-down or stay-up decisions about online speech – on a massive, global scale – have a major impact on freedom of information and, by extension, the democratic rule of law.[10] The most vivid illustration of this impact was unthinkable at the time of our last EU update: Facebook and Twitter denying a sitting US president access to their services; Apple and Google removing the social media app Parler, which had been used to organize the riots, from their app stores; Amazon denying its cloud services to the platform. The resulting fundamental debate about 'de-platforming' was not restricted to US academic and media circles.[11] If anything, the turmoil in the US caused European policymakers to redouble their efforts to 'emancipate' the bloc from American influence.[12] While platforms work to create self-regulatory oversight mechanisms to judge what users should and should not be able to post on their networks, the European Commission's proposal for a Digital Services Act (DSA), discussed in more detail below, shows that the subject of content moderation will be center-stage in the coming years.

Although the role and impact of online services is incomparable to when the E-commerce directive was adopted in 2000, its rules on online service providers' liability, and obligations to be helpful, are still being litigated. Over the past two years, the EU Court of Justice handed down judgments on issues such as the permissibility of preventative filtering measures,[13] the global reach of delisting orders,[14] and the regulatory regime applicable to ride-hailing apps.[15] Facebook, Google, Twitter, Mozilla, Microsoft and TikTok joined forces with advertisers to adopt a European code of conduct against disinformation.[16] During the pandemic, the big tech companies were quick to show responsibility, enacting and enforcing policies against misleading

[9] 'Social media usage in Europe - Statistics & Facts' (Statista, February 10, 2020), https://www.statista.com/topics/4106/social-media-usage-in-europe, consulted on March 25, 2021.

[10] See in more detail: E. Douek, 'Verified accountability: self-regulation of content moderation as an answer to the special problems of speech regulation', Hoover Aegis Paper September 18, 2019 via lawfareblog.com; W. Benedek & M.C. Kettemann, *Freedom of Expression and the Internet (*second edition), Strasbourg: Council of Europe Publishing 2020.

[11] E. Douek, 'Trump is banned, who is next?', *The Atlantic* 9 January 2021; : J. Vincent, 'Zoom cancels talk by Palestinian hijacker Leila Khaled at San Francisco State University', *The Verge* September 24, 2020.

[12] M. Karnitschnig, 'Politico Playbook: What Europe thinks of America after this week', Politico 9 January 2021; R. Fahy et al., 'Deplatforming politicians and the implications for Europe', February 2021, https://www.sectorplandls.nl/wordpress/blog/deplatforming-politicians-and-the-implications-for-europe/.

[13] CJEU 3 October 2019, Case C-18/18 (Glawischnig-Piesczek / Facebook).

[14] CJEU 24 September 2019, Case C-507/17 (Google / CNIL).

[15] CJEU 3 December 2020, Case C-62/19 (Star Taxi App).

[16] https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

information about COVID-19, with mixed results.[17] The all-but-adopted Terrorist Content Regulation allows national authorities to order the removal of online terrorist content.[18] The complexity of the issue did not stop the EU legislature from imposing extremely short take-down deadlines (sometimes within an hour) and setting fines of up to 4% of global turnover.[19] In parallel, the European Commission is preparing legislation to more effectively combat child sexual abuse online.[20]

The emerging landscape of online speech regulation is vast and fragmented. There are more opinions and ways to express them online than humans are able to control. No tech company can have all the content on its service moderated, at least not by humans. No regulator can supervise this process at more than the most macro level. At best, a small fleet of patrol boats is cruising the oceans of online content.[21] Platforms receive a wide variety of notifications, from hideous criminality to difficult edge cases to naked attempts to censor unwelcome-but-legitimate speech.[22] The rules which providers must apply are European, national and internal, spread across an increasingly large range of (mostly thematic) legislative and policy instruments. With the sheer volume of requests, and an intermediary's inherently limited view of the relevant facts, mistakes are par for the course. The largest tech companies have the resources to detect and reject unfounded requests, and litigate them if necessary. Smaller platforms have less resources to spend on automated detection, manual review, and lawyers. They logically opt for a more automated and/or risk-averse course, and will typically move more quickly to take down notified content in case of doubt. Although solid empirical research on overblocking is still scarce, the general picture is clear.[23]

---

[17] Joint Communication 'Tackling disinformation related to COVID-19. Getting the facts right', Brussels 10 June 2020 (JOIN(2020) 8 final) and the reports of online platforms as part of the monitoring program; see also: 'Managing the COVID-19 Infodemic', Joint Statement by WHO, UN and others, September 23, 2020 who.int. A. Knuutila et al, COVID-related Misinformation on YouTube: The Spread of Misinformation Videos on Social Media and the Effectiveness of Platform Policies (COMPROP Data Memo 2020.6), University of Oxford 2020.

[18] Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (2018/0331 COD), adopted by the Council on 16 March 2021 (https://data.consilium.europa.eu/doc/document/ST-14308-2020-REV-1/en/pdf); cf. also Counter-Terrorism Agenda for the EU, December 9,2020, COM(2020) 795 final.

[19] See for a critical discussion of the proposal A. Kuczerawy, 'The proposed Regulation on preventing the dissemination of terrorist content online: safeguards and risks for freedom of expression', December 5, 2018, https://bit.ly/2uD8MtL and D. Keller, 'The EU's terrorist content regulation: expanding the rule of platform terms of service and exporting expression restrictions from the EU's most conservative Member States', cyberlaw.stanford.eu/blog March 25, 2019.

[20] The impact assessment for the proposal has been completed, a public consultation runs through April 15, 2021. See: https://ec.europa.eu/home-affairs/news/fighting-child-sexual-abuse-have-your-say_en. See also: EU strategy for a more effective fight against child sexual abuse COM/2020/607 final, p. 6.

[21] Notice & Takedown systems, supplemented by automated algorithmic checks, still form the basis of combating unlawful and undesirable content. Internet users can report unlawful or undesirable content to online platforms, which then remove the content if necessary. See: T. Gillespie, *Custodians of the Internet; platforms, content moderation, and the hidden decisions that shape social media*, Yale University Press 2018.

[22] D. Keller, 'Empirical evidence of over-removal by internet companies under intermediation liability laws: an updated list', February 8, 2021, see: cyberlaw.stanford.edu/blog.

[23] Id.

Copyright: online use of press publications and liability of upload platforms

One specific, IP-focused intervention in the perceived power of large tech companies can be found in the DSM Copyright Directive (2019/790/EU), which we discussed in our previous update.

Article 15 of the Directive gives press publishers a neighboring right which they can deploy against online use of their press publications by information society service providers. It is subject to the usual exceptions and limitations, and does not apply at all to hyperlinking, private use or – CJEU reference alert – "the use of single words or very short fragments of a press publication".[24] The press publishers' right seeks to address a serious problem – the demise of the traditional revenue model for quality journalism – but does so through a curious and irrational mechanism that is called an IP right but walks and talks like a state aid regime for large press publishers financed by a special tax on tech companies. Time will tell if it can help quality journalism survive.[25]

Article 17 of the Directive provides that a – CJEU reference alert – "provider of an online content-sharing service" is responsible for its users' uploads of protected content, and must therefore obtain authorization from rightholders. The hosting safe harbor set out in Article 14 of the E-commerce directive does not apply, but is replaced by a specific safe harbor in Article 17(4), which applies if the provider demonstrates that it has made "best efforts" to obtain an authorization, and "prevent the availability" of works about which rightholders have provided sufficient information to enable them to do so. This cooperation between platforms and rightholders must protect the rights of both rightholders and users, while simultaneously avoiding overblocking, general monitoring and the identification of individual users. The largest platforms and rightholders may find a way to square all those circles, but the long tail of platforms and rightholders below will struggle to understand their rights and obligations.

Although EU member states must transpose the Directive into their national laws by 7 June 2021, only one country – the Netherlands – has so far completed the necessary legislative procedures. The Dutch transposition is deliberately dull and devoid of any national interpretation, essentially for fear of getting it wrong.[26] By contrast, Germany is trying to put the impossible compromises of Article 17 into workable practice. Its legislative proposal, which is expected to pass into law in May, requires platforms to pay a remuneration to collecting societies for their users' right to upload fragments of protected content in the form of quotations, caricatures, parodies and pastiches, and requires them not to block "presumably authorized"

[24] A.-C. Lorrain, 'Introducing an ancillary right for press publishers: a European law-making ambition for the press - but also on hyperlinking', *Computerrecht* 2020/83.

[25] See e.g. Ben Thompson, 'Publishing is Back to the Future', 27 January 2021 (https://stratechery.com/2021/publishing-is-back-to-the-future/); and 'Media, Regulators, and Big Tech; Indulgences and Injunctions; Better Approaches', 14 May 2020 (https://stratechery.com/2020/media-regulators-and-big-tech-indulgences-and-injunctions-better-approaches/).

[26] Remy Chavannes, 'The Dutch DSM copyright transposition bill: safety first (up to a point)', Kluwer Copyright Blog June 11, 2020 (https://bit.ly/2QKCVp0).

uploads unless rightholders invoke a "red-button procedure".[27] The German approach is creative and detailed, but also expensive and complicated – particularly for smaller platforms. For all its drafters' efforts, we may not know for years whether the EU Court of Justice judges the result to be compatible with the directive.

Media regulation: video-sharing platform services

We discussed the revised Audiovisual Media Services Directive in our previous update.[28] Since then, national transposition laws (belatedly) started entering into force. Video-sharing platform services, which provide access to user-uploaded content over which they do not have editorial responsibility, are now subject to a degree of media-law regulation for the first time. These platforms are now required to take certain measures to protect users, particularly minors, from various types of harmful content. Many platforms which host (some) videos are still not sure whether they qualify as video-sharing platform service, notwithstanding the European Commission's (excessively) broad interpretation of the concept.[29]

Privacy regulation: the right to be forgotten

Since our last update, the EU Court of Justice issued two important judgments about the right of data subjects to have certain search results delisted, also known as the 'right to be forgotten'. In a first ruling, about the territorial scope of a successful removal request, the Court ruled that the GDPR[30] does not contain a basis for an obligation to remove search results worldwide, but does not prohibit it either.[31]

In a second landmark ruling, issued on the same day, the Court dealt with the standard for the delisting of search results that refer to special categories of personal data such as data relating to a criminal conviction.[32] At first sight, the Court takes a strict approach, ruling that the GDPR's ban on processing special personal data should also apply to search engines. However, the Court manages to avoid the seemingly inevitable conclusion that search engines therefore have to deindex all source pages containing information about any natural person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, or criminal convictions and offences (which would include most online news and human-interest content). The Court points to GDPR Article 17(3), which contains an exception to the right to be forgotten when the processing is necessary for the exercise of

[27] See amongst others Paul Keller, 'German government draft on Article 17: Two steps forward, one step back', Communia February 26, 2021 (https://bit.ly/3u83eUt).

[28] Directive 2018/1808/EU of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities.

[29] European Commission, Guidelines on the practical application of the essential functionality criterion of the definition of a 'video-sharing platform service' under the Audiovisual Media Services Directive, (2020/C 223/02).

[30] Strictly speaking, the case fell within the scope of the old Privacy Directive (95/46/EC), but the CJEU implied the GDPR in its judgment to ensure that the judgment is also useful in the future.

[31] CJEU 24 September 2019, Case C-507/17 (Google / CNIL).

[32] CJEU 24 September 2019, Case C-136/17 (GC/CNIL).

freedom of information, and holds that the search engine may refuse a request to be forgotten which concerns special personal data when the display of a search result is strictly necessary for the right to freedom of information of internet users. The judgment makes it clear that right to be forgotten requests will always be a balancing test between privacy on the one hand and the freedom of information on the other.

The European Data Protection Board (EDPB), comprising the 27 EU and 3 EEA EFTA national data protection authorities, published the first part of its guidelines on the right to be forgotten in July 2020.[33] The document is mostly focused on explaining differences between the former Privacy Directive and the GDPR on this topic. The second part, which would include a list of criteria for assessing requests to be forgotten, has yet to be published.

Consumer-protection law goes online

In the past two years, EU consumer-protection law has increasingly focused on online platforms and online sales in general. Consumer-protection law comprises a mishmash of mostly EU law which aims to protect consumers by (i) requiring traders to provide certain information,[34] (ii) prohibiting aggressive or misleading selling techniques,[35] and (iii) providing consumers with certain rights.[36]

Three EU Directives were adopted in 2019, which will have to be transposed into national law in the course of 2021. The Digital Content and Digital Services Directive[37] and the Directive on Contracts for the Sale of Goods[38] form a diptych, giving consumers more information and rights when buying "smart" devices, digital content or digital services. The Modernization Directive, also adopted in 2019,[39] introduces specific obligations for "online marketplaces". These must provide mandatory information about the identity of merchants on the platform; the ranking of products displayed; and whether the marketplace guarantees that reviews actually come from users. The Directive also extends the scope of the legal information obligations to services for which consumers "pay" with their personal data.

[33] EDPB, Guideline 5/2019 on the criteria for the right to be forgotten in the search engine business under the AVG (Part 1) Version 2.0 Adopted on July 7, 2020.

[34] See also Directive 2011/83 on Consumer Rights. Sometimes these obligations to provide information also overlap, resulting in confusion for the parties and the regulator.

[35] Unfair Trade Practices Directive 2005/29.

[36] Consumer Rights Directive and Unfair Terms Directive 93/13.

[37] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, OJ L 2019/136, p. 1.

[38] Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, OJ L 2019/136, p. 68.

[39] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, OJ L 2019/328, p. 7. Also referred to as the Omnibus Directive.

In principle, only the trader is responsible for compliance with consumer-protection law, not the platform which the trader uses. However, in practice, the trader's ability to comply depends in part on the design of the service. That creates a market incentive for platforms to enable compliance, but even then the extent to which a platform can be held responsible raises all sorts of questions: can there be a misleading omission on the part of a trader if there is no space to provide the relevant information in the listing on a shopping comparison service? Can regulators ask Apple to require app providers to prominently display privacy information in the App Store? Can online platforms be required to "de-platform" traders who violate consumer-protection rules?

Digital Services Act

In December 2020, the European Commission stepped into this crowded playing field with a proposal for a major expansion and tightening of the rules for online platforms: the Digital Services Act (DSA).[40] As a regulation rather than a directive, it would upon adoption apply automatically throughout the EU, without transposition by member states and all the potential for subtle or not-so-subtle differences which that entails. The proposal is 45 pages long excluding explanatory memorandum, recitals and financial statement, with 74 detailed articles which the Commission hopes will come into force within two years. While Member States and stakeholders have been providing their initial responses, the European Parliament has been wrangling over which committee will have primary responsibility for the proposal. A massive lobbying fight is looming.

The DSA leaves the E-Commerce Directive of 2000 largely intact, including the under-rated country of origin principle in Article 3.[41] The familiar safe harbors for access, caching and hosting providers, which have enabled both the modern internet and its downsides, will be retained. They are, however, moved into the DSA to prevent national transposition differences. The DSA codifies the CJEU's case law on the safe harbor, and confirms that providers do not lose their entitlement to that safeguard by taking measures themselves to block or remove illegal content (the so-called Good Samaritan dilemma). Article 5(3) contains a quite arbitrary exception to the safe harbor in the situation where a hosting provider, in short, facilitates a remote transaction between consumer and trader in a way that suggests that the provider itself is the trader.

In essence, the DSA retains the ancient foundation of the E-Commerce Directive, and superimposes a mighty new pyramid of further obligations. All hosting providers are presented with a number of rules regarding the processing of complaints about "illegal" content and official

[40] Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825 final dated December 15, 2020.

[41] Recital 33 suggests that the principle does not apply to official orders to remove content or provide information. This seems to us to be incorrect and, moreover, undesirable because it would open the door to official takedown orders based on the different national law of 27 EU member states.

orders to remove information or provide customer data. These rules are fairly basic, but still potentially burdensome, particularly for smaller platforms.[42]

More detailed rules apply to a subset of hosting providers which qualify as an "online platform": a provider of a hosting service which, at the request of a recipient of the service, *stores and disseminates information to the public*. This "dissemination to the public" is not quite the same as "*communication* to the public" in copyright law, although it is defined using similar concepts,[43] which the Court of Justice borrowed from media law 15 years ago and has attempted to explain ever since.[44] In the explanation to its website,[45] the European Commission lists online marketplaces, app stores, sharing economy platforms and social media platforms as examples of online platforms, which shows that this is a very eclectic group of services and thus raises the question of whether it is appropriate to impose exactly the same obligations on them all.

Online platforms face mandatory procedures for complaints and disputes over content removal and account termination. However, those who were critical of the banning of Donald Trump will look in vain for substantive standards for *when* platforms may (or must) "de-platform" content or users. Online platforms must identify certain business customers, long a cherished wish of rightholders but one that may prove unnecessarily laborious for semi-professional users of platforms like Etsy.[46] In processing content complaints, platforms must give priority to – presumably soon to be very numerous – 'trusted flaggers'. They will have additional reporting requirements, for instance on the number of disputes, users, suspensions and the use of automatic content moderation. They will also have to show users real-time information about the origin and targeting of online advertising; some in the European Parliament are calling for a total ban on targeted online advertising.

---

[42] See, for example, the response from the App Association, which advocates for smaller providers of software and online services dated March 30, 2021 (https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-internal-market-and-clarifying-responsibilities-for-digital-services/F2163073).

[43] See Recital 14 DSA: "The concept of 'dissemination to the public', as used in this Regulation, should entail the making available of information to a potentially unlimited number of persons, that is, making the information easily accessible to users in general without further action by the recipient of the service providing the information being required, irrespective of whether those persons actually access the information in question. The mere possibility to create groups of users of a given service should not, in itself, be understood to mean that the information disseminated in that manner is not disseminated to the public. However, the concept should exclude dissemination of information within closed groups consisting of a finite number of pre-determined persons. Interpersonal communication services, as defined in Directive (EU) 2018/1972 of the European Parliament and of the Council, 39 such as emails or private messaging services, fall outside the scope of this Regulation. Information should be considered disseminated to the public within the meaning of this Regulation only where that occurs upon the direct request by the recipient of the service that provided the information."

[44] CJEU December 7, 2006, Case C-306/05 (Rafael Hoteles), referring to CJEU June 2, 2005, Case C-89/04 (Mediakabel).

[45] European Commission, "Digital Services Act: Ensuring greater security and accountability online," https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

[46] See Etsy's reaction of March 31, 2021, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-internal-market-and-clarifying-responsibilities-for-digital-services/F2163497.

The major online platforms ("very large online platforms" or VLOPs) will be subject to additional and far-reaching, systemic supervision. For example, they will have to publish periodically externally verified audits of (their measures to counter) systemic risks of dissemination of illegal content, manipulation and violation of fundamental rights (in particular in relation to the use of content moderation, recommendation systems and targeted advertising). The definition of VLOP in the proposal is based purely on the number of users: an online platform with more than 45 million average monthly users in the EU is a VLOP. A hard, quantitative definition might serve legal certainty, but that certainty is limited because "monthly active users" is subject to interpretation by the European Commission through delegated legislation. Moreover, a hard quantitative trigger discourages medium-sized platforms from growing further, and leaves no room for (some of) the rules to be applied to smaller platforms (or *not* applied to *larger* platforms) based on, e.g., the social risks inherent in the platform's design or business model, or its ability to mitigate those risks. The principle of proportionality should provide some flexibility, but a formalized conditional exemption mechanism would be much better. In any case, one can expect that many of the "bad users" who are ostracized by VLOPs will find refuge with less regulated and less well-equipped non-VLOPs, which will not improve the situation overall.

All these new rules must be enforced. This will be the duty and exclusive competence of the Member State where the provider has its headquarters. A provider offering services in the EU without an establishment in the EU must designate an EU representative and will fall under the jurisdiction of the Member State where that representative is located.[47] The responsible Member State must appoint one or more regulatory authorities, and designate one of them as the "Digital Services Coordinator" (DSC). The DSC must have sufficient independence, resources and powers, and must be able, among other things, to issue "effective, proportionate and dissuasive" fines of up to 6% of annual turnover. VLOPs are subject to enhanced supervision, including serious investigative powers for DSCs and the possibility for the European Commission to intervene if a VLOP breaches its obligations, either at the request of the DSC or, conversely, at the request of other DSCs if the competent DSC is not taking sufficient action.

As an EU regulation, the DSA will have direct effect. Moreover, unlike the GDPR, the DSA leaves little room for further definition or detail at the national level. One question which Member States will have to answer is which supervisory authorities will be charged with enforcing the DSA, and which of them will have the status (in practice perhaps: bear the burden) of being the designated coordinator. Existing regulators for competition law, consumer law, media law etc. are obvious candidates, but which ones and in what relation to each other? In Member States where they exist, it will be hard to overlook the large, well-staffed, converged regulators for competition, telecoms and consumer protection, who are used to enforcing general and sector-specific rules against large companies. After all, the DSA is above all intended to strengthen sector-specific consumer protection. However, media regulators already regulate media and video platforms, and that the DSA derives its urgency primarily from the perceived need to improve the regulation of online *content*. It is also conceivable that Member States will divide supervisory powers among several existing regulators, by subject or even by type of platform. The European umbrella organization of media regulators ERGA, for example, has

[47] See Article 40 in conjunction with 11 DSA. Providers without an EU establishment can thus forum shop, although the question remains who would want to take on the role of representative given that it entails joint liability for fines.

argued that the national media authorities should in any event exercise supervision over online *content* platforms (which, according to ERGA, should then also be extended to cover *undesirable or harmful* content).[48] There are indeed good arguments to give media regulators a role in the application of DSA rules to media platforms, while leaving it to other regulators to enforce with respect to, for example, price comparison services or ride-hailing platforms. We should in any case bear in mind that most national regulators will be playing quite a modest role, since many of the largest platforms currently have their European headquarters in Ireland and will thus be regulated by the Irish regulator(s).

Competition Law

Online platforms continue to be at the centre of European competition authorities' minds. The European Commission kicked off 2019 with another multi-billion dollar fine for Google, this time for Google AdSense for Search, which displays ads around search results on third-party websites. Google had allegedly entered into exclusive agreements with these websites, making it (virtually) impossible for other providers of advertising services to appear in the search results on this website.[49] In addition, the Commission fined the gaming platform Steam for making geo-blocking agreements. [50] The Commission further launched four investigations into Amazon and Apple. The first Amazon investigation is about the use of competitively sensitive information from third-party merchants using the online marketplace.[51] In November 2020, the Commission launched a second investigation into possible preferential treatment of Amazon's own products on the platform.[52] In June 2020, the Commission launched two investigations into Apple. The first investigation concerns the mandatory use of Apple's payment system in the App Store (with 30% commission for Apple),[53] the second denying access to the NFC chip in IPhones.[54]

While regulators have clearly not stopped using competition law against potentially abusive conduct, they have also recognized the limitations of traditional competition law, particularly in

[48] 'ERGA welcomes the DSA and DMA proposals and points out ways for better enforceability', press release with accompanying 'Statement about the European Commission's proposals for a Digital Services Act (DSA) and a Digital Markets Act (DMA)', March 29, 2021, https://erga-online.eu/wp-content/uploads/2021/03/ERGA-DSA-DMA-Statement_29032021.pdf.

[49] European Commission, 'Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising', March 2019.

[50] European Commission, 'Antitrust: Commission fines Valve and five publishers of PC video games € 7.8 million for "geo-blocking" practices', January 2021.

[51] European Commission, 'Antitrust: Commission opens investigation into possible anti-competitive conduct of Amazon', July 2019.

[52] European Commission, 'Antitrust: Commission sends Statement of Objections to Amazon for the use of non-public independent seller data and opens second investigation into its e-commerce business practices', November 2020.

[53] European Commission, 'Antitrust: Commission opens investigations into Apple's App Store rules', June 2020.

[54] European Commission, 'Antitrust: Commission opens investigation into Apple practices regarding Apple Pay', June 2020.

terms of speed.[55] Regulators and legislators alike have mostly come to the conclusion that dynamic digital markets require additional competition-law regulation. Indeed, the conversation has mostly shifted from *whether* there should be additional regulation to *what* these rules should look like.

An early and targeted attempt to level the playing field was made in June 2019 with the Platform-to-Business (P2B) Regulation.[56] The Regulation, which became applicable from July 2020, notably introduces transparency and due diligence requirements for business users of online intermediation services and online search engines. According to its critics, the P2B Regulation did not tackle the problem with sufficient breadth or vigor, failing to impose substantive rules of conduct on online platforms.

The Digital Markets Act (DMA), published in December 2020 together with the DSA,[57] represents a far more radical and ambitious plan to improve the contestability of online markets. We mention three salient features of the DMA:

1. **Determination of platforms to be regulated**. The Commission delineates the companies in the digital sector that fall within the scope of the DMA in the following way. First, the company must offer a "core platform service". This includes online intermediation services (e.g. Amazon), search engines (e.g. Google), social networks (e.g. Instagram), video platforms (e.g. YouTube), number-independent electronic communication services (e.g. WhatsApp), operating systems (e.g. iOS), cloud services (e.g. AWS) and advertising services (e.g. Google Display Network). Second, the provider of a core platform service must qualify as a *gatekeeper*. This is determined using three criteria, all three of which are translated into quantitative benchmarks: i) significant market impact, ii) managing an important gateway for customers, and iii) firmly established and sustainable position.[58] The idea is that this will make it relatively easy for a company to determine for itself whether it will be regulated, but that may be optimistic.

2. **Obligations for gatekeepers**. The DMA contains two detailed lists of obligations for gatekeepers. One list can be applied directly, the other requires further elaboration. The directly applicable list includes a prohibition on combining users' personal data, an obligation to provide price information in advertising services, and a set of obligations aimed at preventing contractual lock-in of business users.[59] The list of obligations requiring further elaboration per platform includes obligations relating to the use of third-party data, apps installed by default, non-discrimination against third-party products, data

[55] As was also established by the European Court of Auditors: 'The Commission's EU merger control and antitrust proceedings: a need to scale up market oversight', November 2020.

[56] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, OJ L 186/2019, p. 57.

[57] Proposal for a Regulation on Contestable and Fair Markets in the Digital Sector (Digital Markets Act) COM/2020/842 final.

[58] DMA, Article 3.

[59] DMA, Article 5.

portability and access to data generated by the platform. Both lists of obligations apply in principle to all gatekeepers.[60]

3. **European Commission and national authorities**. The European Commission has the power to determine gatekeeper status, modify or add to the list of obligations, and impose sanctions if a gatekeeper structurally fails to comply with the obligations (which range from pledges and large fines to, in extreme cases, breaking up the company). The role of Member States in the proposal is limited. Member States are explicitly prohibited from introducing other regulations for gatekeepers that are intended to "level the playing field". The role of national regulators is equally limited, they only have a say on a committee which advises the Commission on its decisions.[61]

Meanwhile, some former and current Member States have already introduced their own regulations. In the UK, the competition regulator has recommended the creation of a specialized regulator, with the power to impose individual codes of conduct on specific platforms.[62] Germany has already gone further, with Parliament approving a proposal empowering the regulator to impose specific prohibitions on certain companies, choosing from a 'menu' of seven – broadly defined – behaviors. What is striking about both initiatives is the freedom, relative to the European proposal, which the national regulator is afforded to impose tailor-made measures.[63]

It remains to be seen how the DMA proposal will develop, after the European Parliament, the Member States and hordes of lobbyists and academics have provided their input. One thing is sure, digital competition law is about to change fundamentally.

What is not changing, at least not for the better, is the definitional jungle of EU platform regulation which drives tech lawyers to despair. New definitions discussed here, such as intermediation service, online platform, very large online platform (DMA), gatekeeper and core platform service[64] (DMA), overlap to an as yet uncertain extent with existing definitions such as *online* intermediation service (P2B Regulation), video-sharing platform service (AVMS Directive), online content-sharing service (DSM Copyright Directive) and number-independent interpersonal communication service (ECC Directive). These are all definitions which determine the scope of application of significantly burdensome regulations. Whether a certain service or service provider falls under a certain definition, and therefore has to deal with particular additional obligations and regulators, will be the subject of disputes and CJEU references for years to come. This has consequences, both for companies which may or may not have to

[60] DMA, Article 6.

[61] Some competition regulators have already spoken out in opposition: 'Give EU nations' antitrust enforcers a role in gatekeeper platform regulation, says Dutch authority's Snoep', MLex, March 2, 2021.

[62] CMA, "Digital Markets Taskforce," December 2020. Available at: https://www.gov.uk/cma-cases/digital-markets-taskforce

[63] GWB-Digitalisierungsgesetz, January 18, 2021, BGB 2021, No. 1, p. 2.

[64] The definition of core platform service, according to Article 2(2) DMA, includes another set of underlying definitions, partly from other regulations and directives: online brokering services, online search engines, online social networking services, video platform services, number-independent interpersonal communication services, operating systems, cloud computing services and advertising services.

comply with the associated rules and for the companies and consumers who the rules are trying to protect. All this uncertainty has a price for the EU's credibility as an exporter of effective tech regulation and breeding ground for the new tech champions of tomorrow.

The emerging European law of data

Open Data and Data Governance

Far from content with the GDPR, European lawmakers are continuing to legislate for the "data-driven economy" with "fair, practical and clear rules" for access to, and use of, data. The goal is to create an internal market for data, allowing data to flow freely but safely across the European Union, through all sectors. The Commission estimates the value of this data economy to be €829 billion by 2025, with 175 zettabytes of data worldwide and over 10 million people employed in the European data sector.[65]

One of the focal points of Europe's digital strategy is access to high-quality data.[66] Since 2013, government bodies have been obliged to make public government information available for reuse, both commercial and non-commercial.[67] That regulatory regime was further strengthened with the Open Data Directive adopted in July 2019.[68] It encourages governments to make dynamic data available via APIs, in real time where possible. It limits public bodies' ability to charge more than marginal costs, invoke sui generis database rights or agree exclusive agreements. There is a new regime for 'high-value data sets', which are considered to be particularly suitable for developing further applications and services and thus bring even greater benefits to society and the economy.[69] The Directive identifies thematic categories within which high-value data sets, to be defined by the European Commission, should be available.[70] The Directive has to be transposed into national legislation by 16 July 2021, but many national transpositions look likely to be late. Meanwhile, in November 2020, the European Commission published its proposal for a Data Governance Act,[71] which aims to further promote reuse with a new regime for 'data intermediaries', rules on the sharing of certain protected data and by facilitating 'data altruism'.[72]

---

[65] European Commission, 'A European Data Strategy', COM(2020) 66 final, February 19, 2020.

[66] See: https://ec.europa.eu/commission/presscorner/detail/en/fs_20_278

[67] Directive 2003/98/EC of 17 November 2003 on the re-use of public sector information, amended by Directive 2013/37/EU of 26 June 2013 on the re-use of public sector information.

[68] Directive 2019/1024 of 20 June 2019 on open data and the re-use of public sector information.

[69] See in particular Chapter V (Art. 2(10)) of the Open Data Directive.

[70] Annex 1 to the Directive provides the categories: geospatial data; earth observation and environment; meteorological data; statistics; businesses and business ownership; and mobility.

[71] European Commission proposal on European data governance (COM(2020) 767, November 25, 2020.

[72] Jay Modrall, EU Data Governance Regulation - A Wave of Regulatory and Antitrust Reform Begins, Kluwer Competition Law Blog November 30, 2020. See also the BNC fiche of 22 January 2021, published on rijksoverheid.nl.

AI Regulation

The EU is also building out the regulatory framework for data, 'big data' and artificial intelligence from other angles. For example, at the request of the European Commission, the University of Amsterdam's Institute for Information Law examined whether the current European IP rules are suitable for artificially created or assisted works or inventions.[73] The researchers found that the current state of AI does not yet allow for fully autonomous creation or invention by computer systems, so that limited adjustments to European copyright and patent law will suffice for the short term. The European Commission adopted the report's conclusions in its recent IP Action Plan.[74]

The European Commission published an overarching AI White Paper in February 2020.[75] As is usual in this genre, it wants to both seize all opportunities and mitigate all risks. The Commission advocates for a risk-based regulatory framework for AI, meaning that AI will be more strictly regulated if it is applied in a sector where significant risks are to be expected and in such a way that significant risks can actually occur. The Commission suggests formulating rules regarding training data; data and registries; transparency; robustness and accuracy; human oversight; and specific regulations for certain AI applications such as remote biometric identification. Based on public responses to the White Paper, the Commission is working on a legislative proposal, which is expected to be published within weeks.[76]

Conclusion

The EU is determined to evolve into a self-aware, digitally sovereign bloc that sets the rules by which global technology companies have to operate. However, it is still struggling to make sharp choices between conflicting objectives, such as between privacy and competition, or between consumer protection and the promotion of innovation. Where the Big Tech debate in the US often seems to revolve around extremes – the absolute limits of the First Amendment, calls to "break them up", regulation through multi-billion-dollar lawsuits – the EU's approach focuses on detailed, problem-specific and increasingly asymmetric market regulation and targeted behavioral remedies. There is much to be said for tailor-made regulation. However, this approach is causing the EU to respond to each perceived problem with separate pieces of legislation, each with its own definitions, rules, and jurisdictional and supervisory structures. The unpredictability and heavy-handedness of the new rules risks entrenching the existing big players who can afford to understand and implement them. While each proposal now comes standard with eye-popping fines to ensure appropriate attention at C-suite level, a coherent, systematically thought-through

---

[73] IvIR, *Trends and Developments in Artificial Intelligence Challenges to the Intellectual Property Rights Framework*, September 2020 (https://www.ivir.nl/nl/ivir-study-for-european-commission-on-ai-and-ip/). See also: Daniel Gervais, 'Is Intellectual Property Law Ready for Artificial Intelligence?', GRUR Int Vol. 69, Issue 2, February 2020; Daniel J. Gervais, 'Exploring the Interfaces Between Big Data and Intellectual Property Law,' *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 2019-3.

[74] European Commission, 'Making the most of the EU's innovative potential - An intellectual property action plan to support the EU's recovery and resilience', COM(2020) 760, November 25, 2020.

[75] European Commission, 'White Paper on Artificial Intelligence - A European approach based on excellence and trust', COM (2020) 65 final, February 19, 2020.

[76] https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence.

EU tech law rulebook is still several MLRC Digital Conferences away. The journey there will be interesting.

Social Media Blocking by Government Officials – Where Does the Law Stand?

By Lyndsey Wajert[1]

I. Introduction

As social media platforms have emerged as a way for political figures and government entities to engage with the constituents and the communities they serve, members of Congress, local police departments, and other government officials have had to navigate not just how to effectively use social media accounts but also how to use them in a way that does not run afoul of the First Amendment. The constitutional question has come into focus over the past few years as a result of courts being called to rule upon First Amendment challenges brought by individuals who have been blocked or censored on social media pages and accounts used by public officials.

The formative case in this area is *Knight Institute v. Trump*, which involved a First Amendment challenge to then-President Trump's blocking of critics from his Twitter account, @realDonaldTrump. 928 F.3d 226 (2d Cir. 2019), *cert. granted, judgment vacated sub nom. Biden v. Knight Inst.*, 141 S. Ct. 1220 (2021). In that case, both the Southern District of New York and the Second Circuit held that a government official using a social media account for official purposes cannot constitutionally block individuals from that account based on their viewpoint. *Knight Inst. v. Trump*, 302 F. Supp. 3d 541 (S.D.N.Y. 2018), *aff'd*, 928 F.3d 226 (2d Cir. 2019), *cert. granted, judgment vacated sub nom. Biden v. Knight Inst.*, 141 S. Ct. 1220 (2021).

Although Trump lost in the lower courts, the case was eventually vacated as moot by the Supreme Court because Trump was voted out of office and no longer a government official. *See Biden v. Knight First Amendment Institute*, 141 S. Ct. 1220 (2021). Aside from a controversial concurrence penned by Justice Thomas that endorsed the idea of treating social media companies as common carriers, the Supreme Court did not wade into the merits of the petition or the decisions below.

And while the Second Circuit's decision in *Knight Institute* can no longer be cited as binding precedent, that court's reasoning has been adopted by the many courts around the country that have been called upon to consider the same questions presented in *Knight Institute*. Those courts have nearly unanimously concluded that public officials who block individuals from their official social media accounts -- based on viewpoint -- violate the First Amendment.

This article examines how the caselaw has developed since the Knight Institute filed the 2017 *Trump* complaint, and what factors courts consider in challenges to social media blocking by public officials. Generally, courts address the following issues: whether the social media account use reflects state action, whether the government has created a public forum, whether the official engaged in viewpoint discrimination when blocking or removing certain comments, whether the government engaged in First Amendment retaliation, and whether qualified immunity precludes

[1] Lyndsey Wajert is a 2020-2021 Legal Fellow with the Knight First Amendment Institute at Columbia University.

the defendant from facing liability for damages. This article will unpack the prevalent legal questions that arise in these cases, as well as analyze the factors used by courts in deciding whether the conduct at issue violates the First Amendment and whether the plaintiff is entitled to relief.

II. Relevant Questions

1. Is the account an official account or a purely personal account?

A court considering a social media blocking case will first determine whether the challenged action implicates state action, as the First Amendment "applies only to the government and not private individuals." *Knight Inst.*, 302 F.Supp.3d 5 at 568. In discerning whether there is state action, the court will analyze whether the relevant social media account is an official, campaign, or personal social media account.

The state action analysis is necessary for both federal officials sued for the deprivation of a user's First Amendment rights, as well as for state officials sued under 42 U.S.C. § 1983 based on the same behavior. Indeed, in Section 1983 actions, the plaintiff "must establish that the [official] acted under color of state law" and that the official's actions "constitute[d] state action." *Attwood v. Clemons*, No. 1:18CV38-MW/MJF, 2021 WL 1020449, at *4 (N.D. Fla. Mar. 17, 2021). Under Section 1983 cases, both color of state law and state action requirements "are treated as the functional equivalent of one another and can be analyzed under the same framework." *Id*.

To begin, social media accounts operated by a government agency or entity, such as a police department or a school district, are indisputably considered to be "an arm of the government entity itself." *Scarborough v. Frederick Cty. Sch. Bd.*, No. 5:20-CV-00069, 2021 WL 419180, at *5 (W.D. Va. Feb. 8, 2021), *reconsideration denied sub nom*, No. 5:20-CV-00069, 2021 WL 1592669 (W.D. Va. Mar. 9, 2021); *see generally Robinson v. Hunt Cty., Texas*, 921 F.3d 440, 449 (5th Cir. 2019) (plaintiff sufficiently pled an official policy of viewpoint discrimination on the county sheriff's office Facebook page), *reh'g denied* (May 16, 2019). However, the question of state action is much more complicated where a social media account is operated by an *individual* government employee because "not every social media account operated by a public official is a government account." *Knight Inst.*, 928 F.3d at 236. In such cases, a court will engage in a "fact–specific inquiry," considering facts like "how the official describes and uses the account," "to whom features of the account are made available," and "how others, including government officials and agencies, regard and treat the account." *Id*. It is not enough for a plaintiff to simply conclude that an account run by a government official constitutes state action. *See Phillips v. Ochoa*, No. 220CV00272JADVCF, 2020 WL 4905535, at *5 (D. Nev. Aug. 20, 2020) (plaintiff "concludes—but has not pled any true facts to show—that [defendant's] conduct about the Facebook page was clothed in the authority of state law.").

In *Knight Institute*, the Second Circuit underscored aspects of the @realDonaldTrump Twitter account that weighed in favor of it being deemed an official account. 928 F.3d at 235–36. Those factors included that the account was "presented by the President and the White House staff as belonging to, and operated by, the President" in both how it appeared and how White House staff described it; that other government offices viewed tweets from the account as official statements

of the president, and that Trump used the account to announce official policies and directives. *Id*. The Second Circuit also noted that Trump used the account to interact with the public and gauge reaction to "what he says and does." *Id*. at 236. This combination of elements rendered the account "an important tool of governance," and thus, subject to the First Amendment challenge. *Id*.

In a case that narrowly predated the Second Circuit's decision in *Knight Institute*, the Fourth Circuit reached a similar conclusion after analyzing similar factors in a Section 1983 action against the chair of the Loudoun County Board of Supervisors. *Davison v. Randall*, 912 F.3d 666 (4th Cir. 2019), *as amended* (Jan. 9, 2019). There, the plaintiff, a Loudoun County resident, alleged that a county official violated his First Amendment and due process rights by blocking him from her Facebook page. *Id*. at 676.

The Fourth Circuit concluded that the official's actions met the color of state law/state action requirement under Section 1983 after considering the "totality of the circumstances surrounding [her] creation and administration of [the page] and [her] banning [of the plaintiff] from that page." *Id*. at 680. The court noted that the official provided information on the page about official activities that she and the county board engaged in, used the page to solicit input from the public on policy issues, and that the page was "swathe[d] in the trappings of her office." *Id*. at 681. More specifically, the "trappings" of the defendant's Facebook page, according to the court, included: (1) posting of her official title on the page; (2) description of the page as belonging to a government official; (3) listing of her government contact information; (4) linking to official government websites; and (5) posting content that had "a strong tendency towards matters related to her office." *Id.* at 680–81.

The Fourth Circuit emphasized that "the specific actions giving rise to [the plaintiff's] claim [were also] linked to events which arose out of [the defendant's] official status." *Id*. at 681. The court noted that the plaintiff was blocked from the page after posting a comment addressing a public county meeting and that the comment "also dealt with an issue related to that meeting and of significant public interest." *Id*. at 681.

In a subsequent case, *Phillips v. Ochoa*, a judge in the federal district court in Nevada analyzed both *Knight Institute* and *Davison*, and "distill[ed] from [them] a non-exhaustive list of questions" that courts consider in determining whether an official acted under the color of state law on a social media account. *Phillips*, 2020 WL 4905535, at *4. The list included: (1) how the account is presented; (2) how the account is used; (3) how the account is categorized; (4) how the account is treated and regarded by others, especially other governmental officials and agencies; (5) to whom the features of the account are made available; and (6) whether the events giving rise to plaintiff's claim arise out of the defendant's official status. *Id*.

Courts faced with the same question as to whether social media account usage reflects state action have generally used a list similar to that discussed in *Phillips*. *See Swanson v. Griffin*, No. CV 20-496 KG/GJF, 2021 WL 930615, at *4–5 (D.N.M. Mar. 11, 2021) (outlining county commissioner's use of individual Facebook page – to discuss meetings, share official letters, comment on policies, and encourage followers to support initiatives – as a rationale for finding that the account was official); *Faison v. Jones*, 440 F. Supp. 3d 1123, 1134 (E.D. Cal. 2020) (describing defendant's profile and banner photographs, defendant's inclusion of his official title

on the page, the discussions of oversight of the sheriff's department, defendant's posting about news and engaging in conversations about the department, and the official nature of plaintiffs' comments); *Garnier v. Poway Unified Sch. Dist.*, No. 17-CV-2215-W (JLB), 2019 WL 4736208, at *7 (S.D. Cal. Sept. 26, 2019) (observing that school board members used their social media accounts to inform public about meetings, share agendas, discuss board events, solicit input from followers on initiatives, all while "swath[ing] their social media pages in the trappings of their office"); *Windom v. Harshbarger*, 396 F. Supp. 3d 675, 684. (N.D.W. Va. 2019) (finding it premature to dismiss litigation but noting that unlike the Facebook page in *Davison*, the account here listed "politician" instead of "public official," featured a private email address and phone number instead of official ones, and that other Fourth Circuit factors weighed "slightly against a finding" that the defendant acted under color of state law).

Although some officials have made creative arguments that their behavior did not constitute state action, courts have largely rejected such arguments. *See Garnier v. O'Connor-Ratcliff*, No. 317CV02215BENJLB, 2021 WL 129823, at *10 (S.D. Cal. Jan. 14, 2021) (rejecting argument that officials did not act under color of state law because they "[were] members of the legislative branch and [could not] take official action outside of a meeting of their legislative body"); *Felts v. Reed*, No. 4:20-CV-00821 JAR, 2020 WL 7041809, at *6 (E.D. Mo. Dec. 1, 2020) (rejecting argument that because there were no ordinances or laws related to the official's Twitter account, his actions could not be under the color of state law), *motion to certify appeal denied*, No. 4:20-CV-00821 JAR, 2021 WL 168746 (E.D. Mo. Jan. 19, 2021); *One Wisconsin Now v. Kremer*, 354 F. Supp. 3d 940, 950 (W.D. Wis. 2019) (rejecting argument that state action must be specifically authorized by a statute as "unworkable, narrow, and, simply put, silly").

2. Is the account an official account reflecting state action or a campaign account?

While the factors promulgated by *Davison* and *Knight Institute* have been adopted by other courts, some courts have had to grapple with the question of not only whether an account is a purely official account or a purely personal account, but whether it is a campaign-related account. Generally, a campaign-related account is considered a personal account for the purposes of the state action analysis, as "[i]t is not enough that the defendant is a public official, because acts that public officials take in 'the ambit of their personal pursuits' do not trigger § 1983 liability." *Campbell v. Reisch*, 986 F.3d 822, 824 (8th Cir. 2021) (citing *Magee v. Trs. of Hamline Univ.*, 747 F.3d 532, 535 (8th Cir. 2014)).

Indeed, the Eighth Circuit Court of Appeals came to this conclusion—albeit over a strong dissent—in a case involving a state legislator's blocking of a constituent from her Twitter account. *Id.* at 826. There, the panel's majority concluded that the defendant's account was "the kind of unofficial account that the [Second Circuit] *Trump* court envisioned," highlighting that the activity on the account primarily focused on her campaign. *Id*. The majority also noted that the defendant "created the account the day she announced her candidacy; she solicited donations to her campaign on the account; and, for over a year, she sought to convince her audience to support her election bid." *Id*.

Not only did the parties in *Campbell* disagree over whether there was state action, but they differed over *how* the court should determine whether the defendant acted under color of state law. The defendant argued that a public employee acts under color of law only "when [s]he

exercise[s] power possessed by virtue of state law and made possible only because the wrongdoer is clothed with the authority of state law." *Id*. at 825 (citation omitted). Under this reasoning, anyone can use the block feature on Twitter, thus the defendant "simply could not have acted under color of state law." *Id*. The plaintiff, on the other hand, argued that keeping with the approach in the *Knight Institute* and *Davison* cases, "for a defendant to act under color of law, her actions need only be 'fairly attributable' to the State, which 'is a matter of normative judgment' whose 'criteria lack rigid simplicity.'" *Id*. citing *Brentwood Acad. v. Tenn. Secondary Sch. Athletic Ass'n*, 531 U.S. 288, 295 (2001).

The majority in *Campbell* ultimately did not decide "which approach is correct," because, "even applying the one [the plaintiff] advance[d], the record [did] not support a conclusion that [the defendant] acted under color of law." *Id*. In distinguishing its decision from the other circuits, the majority explained that the *Knight Institute* and *Davison* courts "were not concerned with distinguishing an official page from a campaign page as we are, and so they [did] not offer much guidance for deciding this case." *Id.* at 827.

The court in *Campbell* appeared to have accepted the same fact-intensive state action inquiry as the courts in *Knight Institute* and *Davison*, though it reached a different conclusion based on the facts there. Other courts have reached similar conclusions. *See Charudattan v. Darnell*, 834 F. App'x 477, 482 (11th Cir. 2020) (noting that the conduct at issue pertaining to defendant's campaign page was not done under color of law because defendant's campaign page "was a private page for [defendant's] reelection, paid for by [defendant], and operated by volunteer off-duty deputies"); *but see Attwood*, 2021 WL 1020449, at *7 (noting, for purposes of summary judgment motion, that a fact finder could reasonably infer that defendant "used his account as a state legislator rather than as a future candidate").

3. Has the government established a public forum or is it engaging in a form of government speech?

Upon finding that social media account usage reflects state action, a reviewing court will then determine whether the government actor/government has created a public forum for speech within the account by "opening an instrumentality of communication 'for indiscriminate use by the general public."' *Knight Inst.*, 928 F.3d at 237 (citation omitted).

In *Knight Institute*, for example, the Second Circuit held that the @realDonaldTrump account constituted a public forum. As the court explained, the Supreme Court specifically held that "social media is entitled to the same First Amendment protections as other forms of media." *Knight*, 928 F.3d at 237 (citing *Packingham v. North Carolina*, 137 S. Ct. 1730, 1735–36 (2017)). Further, the Second Circuit noted that a public forum need not be "spatial or geographic," and "the same principles are applicable" to a metaphysical forum. *Id*. citing *Rosenberger v. Rector & Visitors of Univ. of Virginia*, 515 U.S. 819, 830 (1995). And there are two categories of public fora: traditional public forums and limited (or designated) public forums. *Davison*, 912 F.3d at 681 (citing *Am. Civil Liberties Union v. Mote*, 423 F.3d 438, 443 (4th Cir. 2005)). Fundamentally, "the hallmark of both types . . . is that the government has made the space available—either by designation or long-standing custom—for 'expressive public conduct' or 'expressive activity.'" *Id*. A non-public forum, however, "is one that has not traditionally been open to the public, where opening it to expressive conduct would 'somehow

interfere with the objective use and purpose to which the property has been dedicated.'" *Id*. (citation omitted).

In discerning whether the @realDonaldTrump account constituted a public forum, the Second Circuit looked at "the policy and practice of the government," as well as "the nature of the property and its compatibility with expressive activity," and focused on how the defendants actually used the @realDonaldTrump account. *Knight Inst*., 928 F.3d at 237. The court concluded that the account "was intentionally opened for public discussion when the President, upon assuming office, repeatedly used the [a]ccount as an official vehicle for governance and made its interactive features accessible to the public without limitation." *Id*. Reviewing courts have since found a public forum where officials "chose not to have any privacy settings or content restrictions on [the] page," *Attwood*, 2021 WL 1020449, at *8; and "encouraged, solicited, and allowed public comments," *Windom*, 396 F. Supp. 3d at 683, among other factors. And for social media accounts or pages run on behalf of a government office, courts have considered whether the accounts "[held themselves] out as a platform for unlimited and unrestricted discussion on matters related to [office] operations." *Scarborough*, 2021 WL 419180 at *5.

The Second Circuit rejected the defendants' argument that the @realDonaldTrump account should instead be considered a vehicle for government speech. While "[g]overnmental entities are 'strictly limited' in their ability to regulate private speech in public fora," *Davison*, *912* F.3d at 681 (citing *Pleasant Grove City, Utah v. Summum*, 555 U.S. 460, 469 (2009)), under the government speech doctrine, "[t]he Free Speech Clause does not require [the] government to maintain viewpoint neutrality when its officers and employees speak" about its endeavors. *Knight Inst.*, 928 F.3d at 239 (citing *Matal v. Tam*, 137 S. Ct. 1744, 1757 (2017)). "The Free Speech Clause restricts government regulation of private speech; it does not regulate government speech." *Pleasant Grove*, 555 U.S. at 467. In *Knight Institute*, Second Circuit rejected the government's argument that the @realDonaldTrump account constituted government speech, explaining that while "[e]veryone concedes that the President's initial tweets (meaning those that he produces himself) are government speech," the case "turn[s] on his supervision of the interactive features of the Account." 928 F.3d at 239. The court also noted that "[t]he Supreme Court has described the government speech doctrine as 'susceptible to dangerous misuse,' and that courts should exercise "'great caution' to prevent the government from 'silenc[ing] or muffl[ing] the expression of disfavored viewpoints' under the guise of the government speech doctrine." *Id*. at 239–40 (quoting *Matal*, 137 S. Ct. at 1758).

In *Davison*, the Fourth Circuit observed that the government speech argument "fail[ed] to recognize the meaningful difference between [the defendant's] posts to the [c]hair's Facebook [p]age and the public comments and posts she invited in the page's interactive space," and instead focused on how the county official sought an "exchange of views" from followers of the page in finding a public forum. *Davison*, 912 F.3d at 682, 686. *See also Felts*, 2020 WL 7041809, at *3 ("forum analysis may still apply to the portions of [an] account that are not considered government speech").

Like the Second Circuit in *Knight Institute* and the Fourth Circuit in *Davison*, other courts handling social media blocking cases have largely rejected the government speech argument. *See Anderson v. Hansen*, No. 20-C-1305, 2021 WL 535429, at *9 (E.D. Wis. Feb. 12, 2021) (public

discussion occurring in the Facebook page forum was the participants' speech, not the district's speech); *Faison*, 440 F. Supp. 3d at 1137 (though "defendant's own posts likely qualified as government speech, plaintiffs' comments do not"); *One Wisconsin Now*, 354 F. Supp. 3d at 954–955 (the interactive portion of the Twitter account was severable from the rest of the account and not subject to the government speech exception); *Leuthy v. LePage*, No. 1:17-CV-00296-JAW, 2018 WL 4134628, at *12 (D. Me. Aug. 29, 2018) (plaintiffs stated sufficient facts to plausibly allege that governor's deletion of posts and banning of citizens from his Facebook page does not constitute government speech); *Price v. City of New York*, No. 15 CIV. 5871 (KPF), 2018 WL 3117507, at *14 (S.D.N.Y. June 25, 2018) ("[d]efendants cannot credibly suggest that the public would confuse [p]laintiff's posts criticizing the [c]ity as being the [c]ity's own speech.").

Of course, as noted above, a court engages in a public forum analysis only after determining there is state action. When a court does not find state action, such as for purely personal or campaign-related accounts, the forum analysis does not apply. *See Morgan v. Bevin*, 298 F. Supp. 3d 1003, 1010–11 (E.D. Ky. 2018) ("[Because [defendant] is speaking on his own behalf, even on his own behalf as a public official, 'the First Amendment strictures that attend the various types of government-established forums do not apply."') Indeed, "[n]o one can seriously contend that a public official's blocking of a constituent from her purely personal Twitter account—one that she does not impress with the trappings of her office and does not use to exercise the authority of her position—would implicate forum analysis." *German v. Eudaly*, No. 3:17-CV-2028-MO, 2018 WL 3212020, at *6 (D. Or. June 29, 2018) (quoting *Knight Inst.*, 302 F. Supp. 3d at 569). Therefore, courts conduct the forum analysis as a necessary second step after establishing state action.

4. Has the government engaged in viewpoint discrimination?

Assuming that a social media account qualifies as a public forum, the next question is whether a government actor's conduct in blocking someone from that forum violates the First Amendment. Although the government may place reasonable, viewpoint-neutral limitations on speech in a limited public forum, "viewpoint discrimination, which 'targets' the specific views or opinions of the speaker, rather than the subject matter generally, is 'prohibited in all forums,'" even non-public ones. *Scarborough*, 2021 WL 419180, at *5 (citing *Child Evangelism Fellowship of S.C. v. Anderson Sch. Dist. Five*, 470 F.3d 1062, 1067 n.2 (4th Cir. 2006)). *See also Matal*, 137 S. Ct. at 1763; *Rosenberger*, 515 U.S. at 829 (viewpoint-based restrictions are "egregious" forms of content restriction as the rationale of the restriction is based on suppressing the speaker's ideology, opinion, or perspective).

Having already established that the blocked or deleted speech was indeed protected under the First Amendment,[2] a reviewing court then analyzes whether the official "has blocked [] persons expressing viewpoints he [or she] finds distasteful," *Knight*, 928 F.3d at 239; whether the official sought to "suppress" opinions, *Davison*, 912 F.3d at 687; whether comments critical of policies were deleted by account administrators, *Scarborough*, 2021 WL 419180 at *5; whether officials

[2] The Southern District of New York and other courts have noted that the first step in the social media blocking analysis is usually to determine whether the speech at issue is speech protected by the First Amendment, however, this question is rarely litigated. *Knight*, 302 F. Supp. 3d at 564. For the purposes of this piece, the state action requirement is treated as the first step in the analysis.

censored comments in response to criticism of policies or initiatives, *Windom*, 396 F. Supp. 3d at 684; or whether there is evidence of selective blocking, *One Wisconsin Now*, 354 F. Supp. 3d at 956.

In response to concerns about viewpoint-based blocking, some defendants have asserted that the blocking "did not ban or burden anyone's speech," but this argument has largely been rejected. *Knight Inst.*, 928 F.3d at 238–39. In *Knight Institute*, the defendants argued that because "the only material impact that blocking ha[d] on the [] plaintiffs' ability to express themselves on Twitter [wa]s that it prevent[ed] them from speaking directly to [Trump] by replying to his tweets . . .," the plaintiffs were not burdened. *Id*. The defendants also argued that the plaintiffs were not censored because they could engage in various "workarounds" to access the social media account at issue. *Id*. But as the Second Circuit noted, "burdens to speech as well as outright bans run afoul of the First Amendment." *Id*. citing *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 566 (2011) (stating that the government "may no more silence unwanted speech by burdening its utterance than by censoring its content"). And other courts considering these defense arguments have largely reached the same conclusion. *See Faison*, 440 F. Supp. 3d at 1137–38 ("Regardless of [p]laintiffs' ability to get their message out elsewhere, [p]laintiffs' inability to post on [d]efendant's Facebook page is a burden on their speech."); *Felts*, 2020 WL 7041809, at *5 ("The fact that there exist a number of workarounds, such as creating a new Twitter account, make no difference.").

This is not to say, however, that the government cannot place some restrictions on the speech that occurs in the forum; some restrictions on speech may be acceptable, and courts have not yet weighed in on what restrictions on government-operated social media accounts may pass constitutional muster. But "[t]he government *must* abstain from regulating speech when the specific motivating ideology or the opinion or perspective of the speaker is the rationale for the restriction." *Rosenberger*, 515 U.S. at 829 (emphasis added). Courts will thus consider whether the restrictions are facially viewpoint neutral, *see Robinson*, 921 F.3d at 449–50 (finding sheriff's office's policy regarding Facebook page of "deleting 'inappropriate' comments"' was viewpoint discriminatory, and highlighting that the complaint also alleged that the page "explicitly call[ed] for only "POSITIVE comments regarding the Hunt County Sheriff's Office"); whether the restrictions are made clear to those who post on the page, *see Tanner v. Ziegenhorn*, No. 4:17-CV-780-DPM, 2020 WL 5648642, at *1 (E.D. Ark. Sept. 22, 2020) (noting the parties offered conflicting evidence about when the state police created terms and conditions for the Facebook page, whether the terms were publicly available, and whether the state police targeted comments it disliked); and whether the restrictions have been implemented in a viewpoint-neutral manner, *see Garnier v. Poway Unified Sch. Dist.*, 2019 WL 4736208, at *11 (rejecting summary judgment motion when questions of material fact remained over whether comments were truly disruptive contrary to page policy or whether that was pretext for viewpoint discrimination).

At least one court has accepted certain restrictions where there was no evidence of viewpoint discrimination. *See Charudattan*, 834 F. App'x at 481 (finding no viewpoint discrimination where a sheriff's office's Facebook page had a policy precluding comments that were "clearly off the intended topic of discussion," plaintiff's comment was off topic, and plaintiff failed to show that the office "engaged in a practice of viewpoint discrimination that was 'so well-settled and pervasive that it assume[d] the force of law'"). Courts considering social media blocking

cases may eventually elaborate on other circumstances in which certain restrictions are acceptable.

5. Did the government engage in First Amendment retaliation?

In addition to conducting the above analysis based on viewpoint discrimination, a court reviewing a social media blocking case may also have to consider a First Amendment retaliation claim against an official who has blocked people from an official social media account. "First Amendment retaliation is actionable because 'retaliatory actions may tend to chill individuals' exercise of constitutional rights."' *Constantine v. Rectors & Visitors of George Mason Univ.*, 411 F.3d 474, 500 (4th Cir. 2005) (citing *ACLU of Md., Inc. v. Wicomico County, Md.*, 999 F.2d 780, 785 (4th Cir.1993)).

First Amendment retaliation claims appear to be less common in social media blocking cases. If a plaintiff does raise a First Amendment retaliation claim, however, the plaintiff must show: (1) the plaintiff has a right protected by the First Amendment; (2) the defendant's actions were motivated or substantially caused by the exercise of that right; and (3) the defendant's actions caused the plaintiff some injury. *Dingwell v. Cossette*, No. 3:17-CV-01531 (KAD), 2020 WL 5820363, at *3 (D. Conn. Sept. 30, 2020), *reconsideration denied*, No. 3:17-CV-01531 (KAD), 2021 WL 413619 (D. Conn. Feb. 5, 2021). "With respect to the third element, 'private citizens claiming retaliation for their criticism of public officials have been required to show that they suffered an 'actual chill' in their speech as a result."' *Id*. at *3 (citations omitted). Yet, "[a] plaintiff has standing if he can show *either* that his speech has been adversely affected by the government retaliation or that he has suffered some other concrete harm," which could include "loss of business or some other tangible injury[.]" *Id*.

In *Swanson v. Griffin*, the court determined that the plaintiff pled a plausible First Amendment retaliation claim by alleging facts that showed: (1) the plaintiff "engaged in constitutionally protected activity" by posting on defendant's Facebook page, which was a public forum; (2) the defendant's withholding and destruction of the posts and materials caused the plaintiff "to suffer an injury that would chill a person of ordinary firmness from continuing to engage in the [d]efendant['s] Facebook page"; and (3) the defendant's withholding and destruction of Facebook posts and materials were "substantially motivated" as a response to plaintiff's posts on defendant's Facebook page. *Id.*, 2021 WL 930615 at *6.

And in *Dingwell v. Cossette*, the plaintiff alleged that he was blocked from the Meriden Connecticut Police Department Facebook page after publicly criticizing the police department, though the defendants asserted that the posts that prompted the blocking were "defamatory, inappropriate and harassing." 2020 WL 5820363, at *10. With respect to the retaliation claim, the court found that "genuine issues of material fact remain[ed] in dispute," including "whether the [p]laintiff's posts were protected speech." *Id*. Nonetheless, for the purposes of the decision, the court "assume[d] without finding that the [p]laintiff's posts were protected speech and that the decision to block the [p]laintiff was retaliatory and curtailed his First Amendment rights." *Id*.

6. If the plaintiff's claim is for damages, is the defendant shielded by qualified immunity?

Although many social media blocking cases involve requests for only declaratory and/or injunctive relief, some cases have considered damages claims against government officials sued in their individual capacities, and the corresponding defense of qualified immunity. "The doctrine of qualified immunity protects government officials 'from liability for civil damages insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known.'" *West v. Shea*, No. SACV2001293CJCDFMX, 2020 WL 8269540, at *3 (C.D. Cal. Nov. 12, 2020) (citations omitted).

In evaluating a qualified immunity defense, a reviewing court generally "must determine whether the plaintiff pled facts indicating: (1) the defendant violated a statutory or constitutional right and (2) that right was 'clearly established' at the time of the challenged conduct." *Swanson*, 2021 WL 930615 at *3 (citations omitted). If the court is considering the defense in the context of a Rule 12(b)(6) motion to dismiss by the defendant, and the plaintiff fails to satisfy these prongs, the court can dismiss the claims with prejudice. *Id*.

In *Swanson*, the court ultimately determined that the plaintiff met the first prong for defeating the defendant commissioner's qualified immunity defense, noting that the plaintiff "pled facts and attached evidence" to the complaint that plausibly alleged the defendant "violated the First Amendment by engaging in viewpoint discrimination and retaliation." *Id*. at *5.

The court then moved to the second prong, considering whether the plaintiff pled facts showing that the First Amendment right to be free from viewpoint discrimination and retaliation were "clearly established during the times relevant to the lawsuit." *Id*. at *6. The court noted that "[t]he relevant, dispositive inquiry in determining whether a right is clearly established is whether it would be clear to a reasonable [official] that his conduct was unlawful in the situation he confronted." *Id*. citing *Thomas v. Durastanti*, 607 F.3d 655, 669 (10th Cir. 2010). "[A] preexisting Supreme Court or Tenth Circuit decision, or the weight of authority from other circuits, must make it apparent to a reasonable [official] that the nature of his conduct is unlawful." *Id*. citing *Carabajal v. City of Cheyenne*, 847 F.3d 1203, 1210 (10th Cir. 2017).

Generally, on the second prong, the Supreme Court has instructed courts "not to define clearly established law at a high level of generality." *Id*. Instead "the clearly established law must be 'particularized' to the facts of the case." *Id*. (citations omitted). Further, as the court in *Swanson* noted, "[a]lthough there need not be 'a case directly on point for a right to be clearly established, existing precedent must have placed the statutory or constitutional question *beyond debate*."' *Id*. (citations omitted) (emphasis in original).

The *Swanson* court then looked at Supreme Court precedent on social media such as *Packingham* and well-established caselaw proscribing viewpoint discrimination, and noted that it was "'beyond debate' that a public official violates the First Amendment by using a social media account . . . as a public forum and then engaging in viewpoint discrimination with respect to that account." *Id*. at *7 (citing *Davison*, 912 F.3d at 682). As such, the county commissioner had "fair notice" that his conduct would violate the First Amendment's prohibition on viewpoint discrimination, and the claim survived the defendant's motion to dismiss. *Id*.

The *Swanson* court also considered the qualified immunity defense with respect to the plaintiff's First Amendment retaliation claim and reached the same conclusion. The court noted that the government did not contest the notion that a claim for retaliation under the First Amendment was clearly established in 2020, as a 2007 Tenth Circuit case established the elements of a retaliation claim and the prohibition on viewpoint-based social media blocking was clearly established law by 2019. *Id*. Thus, the court determined that the defendant was not entitled to qualified immunity with respect to the First Amendment retaliation claim, and that claim similarly survived the defendant's motion to dismiss. *Id*. at *6–7.

In *West v. Shea*, another case weighing a motion to dismiss based on the qualified immunity defense, the court was not persuaded that qualified immunity was appropriate at the early stage of the proceedings. In that case, the court found that the plaintiff plausibly alleged that the defendant blocked him from her profile "solely because he expressed a view she did not like" and that "[g]overnmental viewpoint discrimination has long been prohibited by the First Amendment." 2020 WL 8269540, at *4. And though defendant was not entitled to qualified immunity, the court clarified that the "denial of qualified immunity at [that] stage of the proceedings [did] not mean that [the] case must go to trial." *Id*. citing *Keates v. Koile*, 883 F.3d 1228, 1240 (9th Cir. 2018). Instead, the court stated that the defendant could move for summary judgment based on qualified immunity once an evidentiary record was developed. *Id.*

While the courts in *Swanson* and *West* rejected the defendants' qualified immunity defense, other courts have found the defense more persuasive. In *Wagschal v. Skoufis*, the Second Circuit held the defendant was entitled to qualified immunity, reasoning that in August 2018, when the defendant blocked the plaintiff, that act did not violate clearly established law. No. 20-871, 2021 WL 1568822, at *1 (2d Cir. Apr. 22, 2021). "The *Knight* decision was issued nearly one year after [the defendant] blocked [the plaintiff] from the [p]ublic [p]age; accordingly, it was not controlling precedent at the time of [the] allegedly unconstitutional conduct," the court said. *Id*. The defendant was therefore entitled to qualified immunity on the claim for damages. *Id*.

Further, while the plaintiff there asserted that the defendant was not entitled to qualified immunity because the defendant did not "unhide" censored comments until January 2020, almost six months after *Knight Institute* was decided, the court noted that "[e]ven assuming that, after *Knight*'s vacatur, it would remain clearly established that a public official's use of Facebook's tools to hide specific comments on the official's public page violates the First Amendment, such a rule was not clearly established in 2018 by *Knight* or any other decision from our Court or the Supreme Court." *Id*. "Whether hiding comments in this manner would place an unconstitutional burden on speech was not a question addressed by *Knight*, in which we dealt with the President's use of the blocking function on Twitter," the court said, and so the defendant was also entitled to qualified immunity with regard to the damages claim arising from temporarily hidden comments. *Id*.

And like the court in *Wagschal*, the court in *Hyman v. Kirskey* noted that "the governing law wasn't clear enough" when the defendant deleted the posts. No. 3:18-CV-230-DPM, 2019 WL 2323864, at *2 (E.D. Ark. May 30, 2019). That challenge involved the removal of critical comments from the Walnut Ridge Police Department Facebook page, and though the court highlighted *Davison* and *Robinson*, the court noted that those cases were decided *after* the

defendant deleted the posts. *Id*. "The law is still percolating," the court said, and the defendant was entitled to the qualified immunity defense. *Id*.

Thus, the qualified immunity defense appears to be viable in social media cases against individual government officials sued for damages. *See Dingwell*, 2020 WL 5820363, at *3 (accepting defendants' qualified immunity defense and granting their motion for summary judgment); *Attwood*, 2021 WL 1020449, at *14 (while "'principle that a public official may not engage in viewpoint discrimination in a public forum' has been clearly established for years . . . [t]o overcome the qualified immunity defense, citing precedent which established a general right will not do") (citation omitted). It remains unclear, however, whether this defense to damages claims will remain viable as the caselaw continues to develop, and the constitutional right against social media blocking and censorship becomes more established and understood among public officials.

7. Is the case moot?

Finally, courts will consider whether, throughout the course of litigation, a case has been rendered moot. Challenges to blocking or censorship by government officials could potentially be rendered moot by factors such as an official unblocking the plaintiffs, the government restoring previously deleted posts, the official deleting the social media account altogether, or, as demonstrated by *Knight Institute*, the official being permanently suspended from the social media platform or no longer being in office. *See Biden v. Knight Inst.*, 141 S. Ct. 1220 (2021) (citing *United States v. Munsingwear, Inc.*, 340 U. S. 36 (1950)). These factors could feasibly arise during a social media blocking case.

III. Conclusion

The legal landscape emerging in this arena of social media blocking and censorship litigation appears to be one in which the First Amendment largely protects third-party speech on government pages or accounts, though constitutional protection is dependent on a fact-specific analysis on a case-by-case basis. While the law continues to develop, it will be important to watch whether courts expand on the analysis used to discern whether an account is actually a campaign account, whether plaintiffs who have been blocked will bring more claims for First Amendment retaliation, whether plaintiffs will bring more claims for damages, in addition to requests for injunctive and declaratory relief, and whether courts considering qualified immunity defenses will shift toward rejecting such defenses. As public officials, their constituents, and the general public continue to use social media platforms to interact with each other, the courts will continue to face the legal questions discussed here. The hope is that the courts continue to protect the First Amendment in the process.

Managing Compliance with the Growing Patchwork of State Privacy Laws

By Phil Yannella, Kim Phan and Greg Szewczyk[1]

Introduction

Over the past four years, U.S. companies have been forced to expand their compliance programs to comply with an expanding array of international and U.S. state privacy laws. The wave of privacy laws began in May 2018, when the General Data Protection Regulation (GDPR) became effective, triggering new compliance obligations for U.S. companies with operations in the European Union. On the heels of the GDPR, other countries such as Brazil, Australia, India, Canada and China passed or expanded new privacy legislation, further expanding the scope of privacy compliance for U.S. multinationals.

In the U.S., there has likewise been a creeping expansion of state privacy laws. In 2020, the California Consumer Privacy Act (CCPA) became effective, triggering new legal requirements for U.S. companies that conduct business in California and generate yearly revenues of greater than $25,000,000.[2] Other states, such as Nevada, Utah, and Maine, have since passed smaller less comprehensive privacy laws.

In November 2020, California voters approved via ballot initiative, the California Privacy Rights Act (CPRA), which significantly expands on the CCPA and introduced a number of GDPR-like privacy concepts as well as some entirely new legal obligations. In March 2021, the Virginia legislature passed the Virginia Consumer Data Protection Act (VCDPA)[3], which incorporates many of the same concepts as the CPRA, but varies in enough ways that compliance with the CPRA does not necessarily entail compliance with the CPRA.

At the same time, numerous other states have proposed, but ultimately failed to pass state privacy laws. Recently, proposed privacy laws in Florida[4] and Washington[5], for example, failed to pass. The Washington Privacy Act (WPA) has now failed three consecutive years, foundering on the issue of a private right of action – a common point of disagreement in many state legislatures. Presently, other proposed state privacy laws, such as bills in New York and

---

[1] Philip N. Yannella is the Practice Leader of Ballard Spahr 's Privacy & Data Security Group and the firm's Cybersecurity Incident Response Team. He provides clients with 360-degree advice on the transfer, storage, and use of digital information. Kim Phan is a Partner at Ballard Spahr, who counsels clients on federal and state privacy and data security laws and regulations. Her work in this area encompasses strategic planning for companies to incorporate privacy and data security considerations throughout product development, marketing and implementation. Greg Szewczyk is a Partner in Ballard Spahr's Privacy and Data Security and Litigation groups. He has represented companies in cases in numerous privacy and cybersecurity contexts, including data breach class actions, post-incident business-to-business disputes, and alleged violations of laws for online tracking practices.

[2] Cal. Civ. Code § 1798.140(d).

[3] Va. S.B. 1392, § 59-572(A).

[4] HB 969 (proposed Florida Privacy Protection Act).

[5] S.B. 5062 (Washington Privacy Act).

Connecticut, remain alive and could potentially become law in 2021. Due in part to a lack of a federal privacy law – various proposals continue to stalldue to disagreements over enforcement and pre-emption – it is very likely that U.S. states will continue to propose and consider privacy legislation after 2021.

The dilemma for U.S. multinationals is how to manage compliance with the growing patchwork of state and international privacy obligations. These laws, as discussed in more detail in this article, share many characteristics but they each differ in ways that complicate compliance. If privacy law was a Venn diagram, the GDPR would form the outermost ring, with the CPRA, CCPA, and VCDPA fitting within the GDPR in loosely concentric circles. But there is enough variance between these laws that simply complying with the GDPR would not be sufficient for companies subject to all these laws.

The purpose of this article is to compare and contrast the major U.S. privacy laws, identifying areas of overlap as well as areas where compliance will require state-specific analysis, disclosures and policies

Status and Timeline of U.S. State Privacy Legislation and Laws

Since November 2020, two U.S. states – California and Virginia -- have passed comprehensive privacy legislation. The new California law, the CPRA, is essentially a redline and expansion of the CCPA, and will become effective in January 2023. In July 2021, the California Privacy Protection Agency – a first of its kind state privacy regulator created by the CPRA – will announce formal rule making for CPRA regulations.[6] These regulations are expected to be finalized by July 2022. The CPPA will commence enforcement of the CPRA in July 2023. [7]

Virginia's privacy law, the VCDPA, will become effective in January 2023.[8] Unlike the CPRA, however, there is no provision for rule-making in Virginia.

As has become a yearly pattern, numerous other states proposed privacy legislation in 2021, but presently none have passed. Proposed legislation in Alabama, Arizona, Colorado, Connecticut, Illinois, Kentucky, Maryland, Massachusetts, Minnesota, and New York is still under consideration. Legislatures failed to pass proposed privacy legislation in Mississippi, Oklahoma, Florida, Washington, and Utah.

Comparing Different State Approaches to Key Privacy Issues

Compliance Thresholds

Generally speaking, state privacy laws apply to entities that collect personal information from a state's residents in connection with their business operations, plus the satisfaction of certain

6 Cal. Civ. Code § 1798.185(d).

7 *Id*.

8 Va. S.B.1392, § 59-572(A)

qualifying thresholds. One of the key differences between state privacy laws and legislation is what thresholds must be met in order for the laws to apply.

Under the CCPA, those thresholds are set forth in the definition of "business." [9] The CCPA defines business to mean virtually any for-profit entity, including any "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners."[10]

Business is further defined to mean any such entity that "collects consumers' personal information or on the behalf of which that information is collected, and that alone, or jointly with others, determines the purposes and means of processing of consumers' personal information, that does business in the State of California." The CCPA does not define what it means to "do business" in the state.

In addition to the above, an entity is only a "business" under the CCPA if it satisfies one or more of the following thresholds:

- Has annual gross revenues in excess of $25 million;
- Alone or in combination buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 50,000 or more California consumers, households, or devices; or
- Derives 50 percent or more of its annual revenues from selling California residents' personal information.[11]

The CPRA follows the CCPA's model, but it makes important changes that will impact which businesses are subject to the law. The $25 million threshold is the same, but the CPRA specifies that it is measured by the preceding calendar year.[12] The second threshold was changed to 100,000 or more Californian consumers or households (but not devices), and only for those whose personal information is bought, sold, or shared (as opposed to received for a business purpose).[13] The third threshold remains the same.

The VCDPA, using the terminology from the European GDPR, governs the conduct of "controllers" rather than businesses.[14] A controller is defined to mean "the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data."[15] The applicability thresholds are set forth in a specific section dedicated to the

---

9 Cal. Civ. Code §1798.140(c)

10 *Id.*

11 *Id.*

12 Cal. Civ. Code §1798.140(d).

13 *Id.*

14 The VCDPA also uses the GDPR's term "personal data" rather than the CPRA's "personal information."

15 Va. S.B. 1392, § 59.1-571.

scope of the law, which provides that the VCDPA applies to "persons that conduct business in the Commonwealth or produce products or services that are targeted to residents of the Commonwealth and that"

i. During a calendar year, control or process personal data of at least 100,000 consumers (defined to mean a resident of Virginia); or

ii. Control or process personal data of at least 25,000 Virginia consumers and derive over 50 percent of gross revenue from the sale of personal data. [16]

As "process" is defined to mean any operation or set of operations performed on personal data, the first threshold is broader than the CPRA in scope.[17] The second prong's percentage threshold is tied sales of all personal data, and not just sales of Virginia residents. [18] However, the 25,000 component is designed to ensure a certain level of minimum contacts with the state. There is no revenue threshold under the VCDPA.

Other states have generally followed these two models, but with important nuances. For example, the proposed Colorado Privacy Act generally follows the VCDPA model, applying to "controllers" that (i) process the personal data of 100,000 Colorado residents during a calendar year, or (ii) control or process the personal data of 25,000 Colorado residents and derive any revenue from the sale of data.

The proposed Florida Privacy Protection Act (FPPA) has switched between the two models—whereas the initial bill introduced in the House followed the CCPA model fairly closed, the version that passed the Senate closely resembles the VCDPA.[19]

It is widely expected that several more states will continue to propose, advance, and pass privacy legislation. Especially with respect to applicability thresholds, the model chosen will be very significant: under the California model, larger companies that do business nationally will likely be subject under the annual revenue threshold, whereas under the Virginia model, such companies may not be subject if they do not have a significant presence in that state. In the media context, this difference could be particularly significant when serving a relatively small number of consumers outside of the state of primary broadcast or publication.

Exclusions and Exemptions to Compliance

Differences in the substance and scope of exclusions will also play a significant role in whether or how state privacy laws apply. For example, the CCPA and CPRA exclude personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley

---

16 § 59.1-572(A).

17 § 59.1-571.

18 *Id.*

19 Although both the Florida House and Senate passed competing versions of this bill, the two chambers were unable to reach consensus on a final bill before the close of the legislative session on April 30, 2021.

Act ("GLBA").[20] GLBA-regulated financial institutions therefore do not have to comply with the CCPA and CPRA for personal information regulated by the GLBA, but they do have to comply with the CCPA and CPRA for other sets of personal data.

Complying with these different standards for different data can obviously cause operational difficulties. The VCDPA, on the other hand, provides full exclusions for financial institutions subject to the GLBA.[21] Differences in the scope and extent of exclusions relating to HIPAA and the FCRA will be similarly important in those industries.

Four types of exclusions are likely to have significant impacts on the media industry: (1) exclusions for business-to-business data; (2) exclusions for employees; (3) exclusions relating to publicly available information; and (4) exclusions for non-profit organizations.

The CCPA, the CPRA, and the VCDPA all provide exclusions for personal information collected and processed in the business-to-business context. The VCDPA accomplishes this exclusion through its definition of "consumer," which "does not include a natural person acting in a commercial or employment context."[22] The CCPA and CPRA accomplish it through exemption provisions, which are currently set to expire on January 1, 2023, although it is widely believed that the provisions will be extended and/or renewed.[23]

With respect to employee personal information, the VCDPA provides a full exclusion through its definition of "consumer," whereas the CCPA and CPRA provided limited exclusions that still require businesses to provide some notices to employees, job applicants, contractors, officers, and directors. As with the business-to-business exclusion, the CPRA employee exclusion is set to expire but is expected to be extended.

The different treatment that may be afforded to publicly available information is another area that may be of particular importance to media companies. For example, under the CPRA, personal information is defined to exclude "consumer information that is . . . [p]ublicly and lawfully available information reasonably believed to be made available to the public in a lawful manner and without legal restrictions."[24] "Publicly available" is defined to include information that is lawfully made available to the general public "from a widely distributed media."[25] The Florida bill contains a similar provision. The VCDPA defines "sale of personal data" to exclude "[t]he disclosure of information that the consumer (i) intentionally made available to the general public via a channel of mass media and (ii) did not restrict to a specific audience."[26] Nuances in factual scenarios may have important consequences, so media companies should take particular

---

20 Cal. Civ. Code §1798.145

21 Va. S.B. 1392, § 59.1-572(B).

22 § 59.1-571 (defining consumer)

23 Cal. Civ. Code §1798.145.

24 Cal. Civ. Code § 1798.140(v)(2).

25 *Id.*

26 Va. S.B. 1392, § 59.1-571

care in analyzing the impact of how personal information is collected in the newsgathering process.

Finally, all of the privacy laws that have passed to date have excluded non-profit organizations from their scope.[27] However, non-profit media organizations should not assume this will be the case for all future bills, as the proposed Washington Privacy Act[28]—which failed to advance in recent weeks—would have applied to non-profits starting in 2026. Accordingly, it is important for non-profit media organizations to stay apprised of state privacy laws, and potentially begin building compliance regimes in some areas of their operations.

Data Minimization Principles

While much of the available guidance had already suggested that organizations minimize the data they collect and store, the new privacy laws impose statutory obligations on subject companies to minimize data collection and use.

For example, the CPRA provides that a "business's collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected."[29] The VCDPA provides that a controller shall "[l]imit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed" and prohibits businesses from processing personal data "for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data is processed."[30]

Media companies and digital platforms/technology companies should begin considering and adopting policies to allow compliance with these requirements, including analyzing the scope of the business purpose for which personal data is collected. For example, when collecting personal data as part of the newsgathering process, the company may wish to specify whether such data is being collected and processed solely with respect to that story, or whether it is collected and processed for a broader substantive issue that may allow broader use.

Data Protection and Privacy Risk Assessments

Many companies are already performing data security risk assessments on an annual basis. However, the new privacy laws may impose an obligation to incorporate privacy risk assessments into a company's procedures—including with specific criteria in a written document that is discoverable by state regulators. For organizations that are not subject to the European GDPR, the privacy assessment requirements may be a new concept.

Under the CPRA, businesses whose processing presents a significant risk to consumers' privacy or security will be required to (1) conduct an annual cybersecurity audit, and (2) submit to the

---

[27] § 59.1-572(B); Cal. Civ. Code, § 1798.140(d).

[28] S.B. 5062 (Washington Privacy Act)

[29] Cal. Civ. Code § 1798.100(c).

[30] Va. S.B. 1392, § 59.1-574.A.1-2.

newly formed California Privacy Protection Agency a risk assessment with respect to their processing of personal information.[31] The CPRA does not specifically define what constitutes a significant risk, but it does state that factors to be considered include the size and complexity of the business and the nature and scope of processing activities.

The risk assessment must weigh the benefits of processing to the business, consumers, other stakeholders, and the general public, against the potential risks to the rights of the consumers.[32] This balancing must be done with the goal of restricting or prohibiting the processing if the risks to the privacy of the consumer outweigh the benefits. The risk assessment must be provided to the newly formed Agency "on a regular basis."[33] The new Agency will be issuing regulations, so businesses will likely gain better clarity on the frequency and substantive requirements of the privacy risk assessment. [34]

Under the VCDPA, all controllers are obligated to perform and document a data protection assessment for each of five identified processing activities: (1) processing for targeted advertising; (2) processing for sales; (3) processing for profiling where there are specific types of foreseeable risks; (4) processing sensitive data; and (5) processing that involves personal data that presents a heightened risk of harm.[35] The data protection assessment must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. [36]

The VCDPA provides that the Attorney General can request, pursuant to an investigative civil demand, that a controller disclose any data protection assessment that is relevant to an investigation, and the controller must make the data protection assessment available.[37] However, the VCDPA specifically provides that any disclosed data protection assessment will not be subject to public inspection under the Virginia Freedom of Information Act, and that production does not waive any applicable attorney-client privilege or work product protection.[38]

Enforcement and Civil Liability

One of the most important differences in state privacy laws is whether there is a private right of action. Indeed, one of the most common reasons why proposed state privacy laws have failed to pass is because of a failure to arrive at a consensus with regard to a private right of action.

---

31 Cal. Civ. Code § 1798.185(a)(15).

32 *Id.*

33 *Id.*

34 *Id.*

35 Va. S.B. 1392, § 59.1-576

36 *Id.*

37 *Id.*

38 *Id.*

The CCPA, which will remain in effect until January 2023, when the CPRA becomes effective, has a private right of action.[39] Plaintiffs have the right to collect the greater of actual damages or between $100 and $750 in statutory damages, per consumer per incident. The CPRA continues the CCPA's private right of action with statutory damages for data breaches caused by a business's failure to maintain reasonable security measures. The VCDPA expressly states that it does not create a private right of action.[40]

The CPRA will be enforced by the newly created California Privacy Protection Agency, which will have the ability to seek $2,500 per violation, or $7,500 for intentional violations or violations involving minors.[41] The Agency will be able to do so in administrative actions.

The VCDPA will be enforced by the Virginia Attorney General, who will be able to seek up to $7,500 per violation, plus reasonable expenses and attorneys' fees.[42]

The key issue likely to determine whether more states pass privacy laws is the degree to which state legislatures are able to arrive at a consensus with regard to the private right of action.

Consumer Disclosures

Transparency has long been an essential principle to the protection of consumer privacy. The CCPA requires that a company with an online privacy policy must include a description of consumer privacy rights, a list of the categories of personal information it has collected about consumers in the preceding 12 months, and if applicable, a list of the categories of personal information it has sold or disclosed about consumers in the preceding 12 months. [43] In addition to prescribing the content of these consumer disclosures, the CCPA regulations also require that any consumer disclosures be in easy-to-read plain language, formatted to draw consumer attention, be displayed in the same language as a company's marketing materials, be accessible to those with a disability, and be provided in a clear and conspicuous manner whether presented online or offline.[44]

Similarly, the VCDPA requires that companies provide consumers with a privacy notice that must include the categories of personal data processed by the controller, the purpose for processing personal data, how consumers may exercise their consumer rights, the categories of personal data that the controller shares with third parties, the categories of third parties with whom the controller shares personal data, and whether a controller sells personal data to third parties or processes personal data for targeted advertising.[45]

---

39 Cal. Civ. Code § 1798.150.

40 Va. S.B. 1392, § 59.1-579, 580.

41 Cal. Civ. Code § 1798.199.90

42 Va. S.B. 1392, § 59.1-579, 580.

43 Cal. Civ. Code § 1798.199.90

44 CCPA Reg. § 999.304(a), 308.

45 Va. S.B. 1392, § 59.1-574(C).

Consumer Rights

The ability for consumers to exercise some level of control over the collection, use, and sharing of their personal information has been embodied in state privacy laws as various consumer rights. As observed in California, Virginia, and in the various state privacy legislative proposals that have been introduced so far in 2021, these consumer rights generally fall into the following broad categories:

- Right to Access (know what personal information a company has collected)
- Right to Correct (direct a company to resolve inaccuracies in personal information)
- Right to Delete (direct a company to permanently destroy personal information)
- Right to Restrict Use (limit the ability of a company to use personal information)
- Right to Portability (transfer of personal information to another party)[46]

State privacy laws generally require that companies provide consumers with easily accessible means to exercise these consumer rights, subject to verifying and/or authenticating the identity of the consumer making the request.

Vendor Obligations

Vendors often have access to the personal information of consumers in their role providing various services to companies. Thus, state privacy laws have extended consumer privacy protections to these third parties. Some states, like Virginia, have modeled these third-party requirements in a manner similar to the GDPR by designating an entity as a "controller" or a "processor."[47] Other states are following the standard set by the CCPA and designated an entity as a "business" or a "service provider."[48] Regardless of the terminology, it is clear that states intend to impose privacy obligations to downstream recipients of consumer personal information.

The CPRA requires that prior to sharing any consumer personal information, a business must enter into a written contract with a service provider that:

- Specifies the limited and specified purpose for selling/disclosing personal information;
- Requires the same level of privacy protection as those imposed on the business;
- Grants the business audit rights on any downstream uses of personal information by the service provider;

---

[46] Va. S.B. 1392, § 59.1-573; Cal. Civ. Code § 1798.110-121.

[47] Va. S.B. 1392, § 59.1-575.

[48] Cal. Civ. Code § 1798.110-40(v),(w).

- Requires the service provider to provide notification to the business if the service provider can no longer comply with CPRA; and

- Grants the business the authority to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information by the service provider.[49]

Similarly, under the VCDPA, a controller must enter into a written contract with any third-party processors that set forth:

- Instructions for processing personal information;

- The nature and purpose of any personal information processing;

- Types of personal information that will be subject to processing;

- The duration of any processing;

- Subject to a duty of confidentiality, an obligation to delete or return personal information when the relationship between the controller and processor terminates; and

- An affirmative obligation to provide necessary information as part of any data protection assessments being conducted in compliance with the VCDPA.[50]

Due to the lengthy amount of time required to negotiate and finalize amendments to vendor agreements, companies should be planning ahead to incorporate these new contract clauses in a timely manner ahead of the January 1, 2023 effective date for both the CPRA and the VCDPA.

Financial Incentives

As previously discussed above, state privacy laws prohibit companies from discriminating against or otherwise penalizing consumers who choose to exercise their privacy rights. Such discrimination could take any one of the following forms:

- Denying goods or services to the consumers;

- Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties;

- Providing a different level or quality of goods or services to the consumers; or

- Suggesting that the consumers will receive a different price or rate for goods or services or a different level or quality of goods or services.

---

[49] § 1798.100(d).

[50] Va. S.B. 1392, § 59.1-575.

However, financial incentives or other benefits can be provided to consumers without violating this prohibition, subject to certain conditions. In California, businesses must provide consumers with a notice of financial incentive that describes the material terms of any financial incentive program so that a consumer may make an informed decision about whether to participate. [51] Consumers must provide opt in consent to any such financial incentive program and must be able to withdraw from the program at any time.[52] The CCPA regulations also require that any notice of financial incentive explain how the financial incentive or price or service difference is reasonably related to the value of the consumer's data, including: a good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and a description of the method the business used to calculate the value of the consumer's data.[53] The CCPA prohibits any financial incentive that would be unjust, unreasonable, coercive, or usurious.

The CPRA states that, "Consumers should benefit from businesses' use of their personal information" and expressly contemplates financial incentive programs like loyalty, rewards, discount, or club card programs.[54] VCDPA does not set forth the detailed requirements of the CCPA, but Virginia does require voluntary participation to opt in to such programs.[55] As other states enact privacy laws, the various requirements associated with financial incentive programs may vary, but it seems clear that a path forward for these types of programs will likely be incorporated into any new state laws.

Opt Outs and Consents

One of the most complicated areas of privacy compliance relates to management of differing state requirements for opt-outs and consents for the sale or sharing of personal information. The CCPA requires an opt-out for the "sale" of personal information.[56] The CPRA expands this right and includes a required consumer opt-out for the "sharing" of personal information.[57] The

---

51 Cal. Civ. Code § 1798.125(b).

52 *Id.*

53 The CCPA regulations provide the following examples of how a business can calculate the value of consumer data: (1) The marginal value to the business of the sale, collection, or deletion of a consumer's data. (2) The average value to the business of the sale, collection, or deletion of a consumer's data. (3) The aggregate value to the business of the sale, collection, or deletion of consumers' data divided by the total number of consumers. (4) Revenue generated by the business from sale, collection, or retention of consumers' personal information. (5) Expenses related to the sale, collection, or retention of consumers' personal information. (6) Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference. (7) Profit generated by the business from sale, collection, or retention of consumers' personal information. (8) Any other practical and reasonably reliable method of calculation used in good faith.

54 Cal. Civ. Code § 1798.125(b).

55 Va. S.B. 1392, § 59.1-574(A)(4).

56 Cal. Civ. Code § 1798.120.

57 *Id.*

CPRA also provides consumers with a limited right to opt out of the processing of "sensitive personal information."[58]

Virginia similarly requires an opt-out for the sale of personal information as well as the sharing of personal information for "targeted advertising." Virginia, unlike California, requires a consumer consent for the processing of "sensitive personal information."

The reason compliance with these opt-out and consent rules is so complicated lies in the different definition of key terms such as "sensitive personal information," "sale", and "targeted advertising."

Definition of Sale

The CPRA adopts the CCPA's definition of sale, which requires the sharing of personal information to a third party for monetary "or other valuable consideration". What "valuable consideration" means is not defined under either law and has been a source of significant legal debate under the CCPA, particularly in the context of behavioral advertising. Virginia, by contrast, defines sale exclusively to require monetary consideration.

As with other areas of privacy law, California's and Virginia's approach toward the definition of sale have become the dominant models for other proposed privacy laws. The WPA and the FPPA – both of which failed this year – follow the California model. Nevada, by contrast, follows the Virginia model.

Definition of Sensitive Personal Information

The CPRA (but not the CCPA) provides consumers with a limited right to opt-out of the processing of sensitive personal information.[59] The limited nature of the right may explain the law's very long list of what constitutes sensitive information, which includes "social security number, driver's license number, state identification number, passport, financial account number, credit card number, precise geolocation, racial and ethnic information, religious or philosophical belief, union membership, genetic data, the contents of text or email messages unless read by the intended recipient, biometric data, sexual orientation or sex life."[60]

By contrast, Virginia's privacy law requires affirmative consent prior to the processing sensitive personal information, but defines the term much more narrowly. Under the VDCPA, sensitive personal information is race/ethnic information, religious affiliation, medical diagnosis, genetic data, biometric data precise geolocation, personal information of a minor, sexual orientation, citizenship or immigration status. [61] It remains to be seen how much of an operational impact these new consent requirements will have on media companies and digital platforms/technology companies subject to the VDCPA because, with the exception of precise geolocation, most of the

---

58 § 1798.121.

59 *Id.*

60 § 1798.140(ae).

61 Va. S.B. 1392, § 59.1-571.

data defined as sensitive would not be automatically collected by websites or apps but would typically require the completion of forms or surveys, which often include express consents already.

The Definition of Consent

One area of commonality among recently passed, as well as proposed but defeated, privacy laws is the definition of consent. Both the CPRA and the VDCPA define consent to require affirmative actions.[62] The CPRA definition of consent is as follows: "'Consent means any freely given, specific, informed and unambiguous indication of the consumer's wishes by which he or she, or his or her legal guardian, by a person who has power of attorney or is acting as a conservator for the consumer, such as by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to him or her for a narrowly defined particular purpose. Acceptance of a general or broad terms of use or similar document that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through dark patterns does not constitute consent."[63]

The requirement of affirmative action to signal consent is similar to the GDPR, and stands in stark contrast to other U.S. privacy laws, such as the TCPA or the Wiretap Act, which allow consent to be implied by consumer conduct. The CPRA's reference to dark patterns reflects growing regulatory concern with the use of deceptive interfaces to manipulate consent. What "dark patterns" means is not currently defined, and bears close monitoring.

Definition of Targeted Advertising

The CPRA expands on the CCPA by providing consumers with a new opt-out for the sharing of personal information. "Sharing", however, is defined to refer to sharing for the purposes of "cross contextual behavioral advertising,"[64] which is further defined to mean "the targeting of advertising to a consumer based on the consumer's personal Information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts."[65]

The VDCPA similarly provides an opt-out for targeted ads, but defines "targeted advertising" to mean the display advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests."[66] Notably the definition does not include contextual ads, first-party ads, consumer's request for information

---

62 The WPA and FPPA included similar definitions of "consent."

63 Cal. Civ. Code, § 1798.140(h).

64 § 1798.140(ah).

65 § 1798.140(k).

66 Va. S.B. 1392, § 59.1-571.

or feedback or the processing personal data solely for measuring or reporting advertising performance, reach, or frequency.

Even before the passage of these laws, adtech models were in a state of flux with Google moving away from allowing tracking cookies, and Apple requiring that app developers obtain consent prior to enabling tracking on applications available through the Apple Store. What adtech models will rise in place of the tracking cookie, and whether those models will fall within the definition of targeted advertising is an issue U.S. companies will need to carefully monitor.

Automated Profiling

Another area of commonality among the CPRA and the VDCPA (as well as other proposed, but defeated U.S. state privacy laws) is with regard to automated profiling. This is yet another concept borrowed from the GDPR, and is intended to protect consumers from the potential downside of algorithmic profiling.

Both the CPRA and VCDPA laws define "profiling" to cover any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.[67] The VDSPA provides an opt-out for profiling that has a "legal effect."[68] What "legal effect" means is not defined under the law, and bears close monitoring by U.S. companies. The CPRA expressly delegates rule-making to the CPPA to address profiling of consumers.[69]

Recommendations for Managing Compliance

How then should U.S. companies, particularly media companies and digital platforms/technology companies, that may be subject to multiple overlapping privacy laws manage compliance?

As an initial matter, companies should determine what laws actually apply to them. There are differing thresholds for compliance under the Virginia and California laws (to say nothing of the GDPR). Assuming a company hits a threshold trigger for compliance, the next question is the extent to which the company can avail itself of exclusions, particularly exclusions for employees and B2B transactions. After scoping the areas of data subject to privacy laws, companies should next determine the extent to which their obligations will vary under applicable laws. For example, an opt-out may be required in California but not Virginia for the same kind of processing activity. The answer to this question then raises another question: should companies strive for compliance with the most restrictive law where privacy laws overlap or address compliance at the state level?

---

67 Va. S.B. 1392, § 59.1-571; Cal. Civ. Code § 1798.140(z)

68 Va. S.B. 1392, § 59.1-573(A)(5).

69 Cal. Civ. Code § 1798.185(C)(16)

Some of the core compliance projects that companies may need to pursue include (1) data mapping – in particular mapping sharing activities, profiling, high risk activities, and characterizing vendors; (2) revising record retention programs to address new data minimization requirements; (3) revising vendor contracts; (4) assessing opt-out and consent requirements, which maybe a very granular analysis; and (5) assessing the extent to which the company can avail itself of any legal exemptions from privacy obligations.

Issues that companies should continue to monitor include: the status of rule-making in California – which is likely to significantly impact operations decisions – likely revisions to the VCDPA; the passage of additional state privacy laws; changes in behavioral advertising models that may or may not trigger the need for opt-outs; and the adoption at the corporate level of new automated technologies involving consumer data that may constitute profiling.

Die Hard: Will Constitutional Roadblocks and a Lack of Consensus Stall Section 230 Reform?

By Ambika Kumar, Robert Miller, and Sarah Burns[1]

Introduction

The internet would not be what it is today without Section 230, 47 U.S.C. § 230, enacted in 1996 as part of the Communications Decency Act (CDA). The statute effectively protects online platforms from potential liability of traditional publishers—for defamation and the like—for content provided by users and other third parties. Courts have expansively interpreted this immunity to bar most claims attempting to hold online service providers responsible for user content, and Section 230 is widely credited as enabling the proliferation of online content. [2]

In recent years, however, elected officials, courts, and others have raised concerns about the statute. Some have focused on how it permits providers to disseminate unlawful content, such as harassment and hate speech, without consequence. Others complain that Section 230 purportedly allows providers to discriminate against disfavored viewpoints by choosing what content to block or remove. Former President Trump, who subscribed to the latter position, put his view bluntly: "REPEAL SECTION 230!!!"[3] President Biden has also expressed interest in reviewing the law.[4]

Bipartisan and divergent concerns over what providers allow—or disallow—on their platforms have resulted in a rash of proposals to limit Section 230's scope. Congress has enacted only one such limit, in 2018, which resulted in constitutional challenges and self-censorship.[5] Many more are pending, but it has proven exceedingly difficult to reach agreement on reform—and even more difficult to tweak Section 230 without threatening to reshape the online landscape. This article reviews the background and evolution of Section 230, explains proposals to reform or eliminate it, and evaluates some First Amendment implications of those proposals.

---

[1] Ms. Kumar is a partner and Mr. Miller an associate in the Seattle office of Davis Wright Tremaine LLP. Ms. Burns is an associate in the firm's Los Angeles office. The following partners in the firm's Washington, D.C., office, also provided valuable input: Robert Corn-Revere, David Gossett, and Christopher Savage.

[2] *See* Jeff Kosseff, The Twenty-Six Words That Created the Internet (Cornell University Press 2019).

[3] Oct. 6, 2020 tweet, available at https://www.thetrumparchive.com/.

[4] *Top Democrat speaks to Biden staff about key internet law*, Reuters, March 22, 2021, available at https://www.reuters.com/article/us-usa-democrat-tech/top-democrat-speaks-to-biden-staff-about-key-internet-law-idUSKBN2BE2EG.

[5] *See infra* n. 26-43 and accompanying text.

How We Got Here

Goals and Enactment of Section 230

Section 230 grew out of early internet censorship efforts, which some activists referred to as the "Great Internet Sex Panic of 1995."[6] The primary purpose of the proposed legislation that became the CDA "was to protect children from sexually explicit internet content."[7] The core provision, drafted by Senator James Exon, criminalized sending or showing obscene or indecent content to minors online.[8] As part of a compromise intended to avoid direct government regulation of content, the House of Representatives added an amendment—including what became Section 230—that became part of the Senate bill that became the Telecommunications Act of 1996. The Telecommunications Act was an omnibus reform of the Communications Act of 1934, to "maintain the robust nature of internet communication and, accordingly, to keep government interference in the medium to a minimum."[9] Just a year after Congress enacted the CDA, however, the Supreme Court struck down the criminal provisions.[10] Only Section 230 survived.

One primary focus of Section 230 was to overrule a New York trial court decision which held that an online service provider could be treated as the publisher of, and thus liable for, content its users posted.[11] The court relied heavily on the facts that the provider advertised its practice of controlling content on its service and actively screened and edited material posted on its message boards. The *Stratton Oakmont* approach left providers with a "grim choice": A provider that voluntarily filtered content would be responsible for all posts, while "providers that bur[ied] their heads in the sand and ignore[d] problematic posts would escape liability altogether."[12]

---

[6] *See* Sarah Jeong, *How panics about pictures of naked women shaped the web as we know it*, The Washington Post, Aug. 19, 2016, available at https://www.washingtonpost.com/posteverything/wp/2016/08/19/how-panics-about-naked-pictures-of-women-shaped-the-web-as-we-know-it/.

[7] *Force v. Facebook, Inc.*, 934 F.3d 53, 63 (2d Cir. 2019), *cert. denied*, 140 S. Ct. 2761 (2020).

[8] *See* Sarah Jeong, *How panics about pictures of naked women shaped the web as we know it*, The Washington Post, Aug. 19, 2016, available at https://www.washingtonpost.com/posteverything/wp/2016/08/19/how-panics-about-naked-pictures-of-women-shaped-the-web-as-we-know-it/; Ambika Kumar, *The Test of Time: Section 230 of the Communications Decency Act Turns 20*, Media Law Monitor, Davis Wright Tremaine LLP, available at https://www.dwt.com/blogs/media-law-monitor/2016/08/the-test-of-time-section-230-of-the-communications.

[9] *Force*, 934 F.3d at 63; *see* Ken S. Meyers, *Wikimmunity: Fitting the Communications Decency Act to Wikipedia*, 12 Harv. J. L. & Tech., at 172-73, available at https://poseidon01.ssrn.com/delivery.php?ID=756021072024121107121084093000031069015032009051054004022005113025030125094098071078007052003023030014055081113099098090077021004026083033014126083125090079070064083035082095095083102009073083088097022072087091126111123092066027074010078073105126&EXT=pdf&INDEX=TRUE.

[10] *Reno v. Am. Civil Liberties Union*, 521 U.S. 844 (1997).

[11] *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710, at *6 (N.Y. Sup. Ct. May 24, 1995).

[12] *Fair Hous. Council v. Roommates.com, LLC*, 521 F.3d 1157, 1163 (9th Cir. 2008).

Section 230 addresses this concern through two substantive protections. The first, Section 230(c)(1), commonly described as The Twenty-Six Words That Created the Internet,[13] provides: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." The other, Section 230(c)(2), addresses the rights of platforms to restrict content, and states "no provider or user of an interactive computer service shall be held liable on account of… (a) any action taken voluntarily in good faith to restrict access to… material that the provider or user considers… objectionable… or (b) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in [subparagraph (A)]." (Other provisions of Section 230 provide that "no liability may be imposed under any State or local law that is inconsistent with this section,"[14] and exempt (among other things) intellectual property laws and federal criminal statutes.[15]

Application of Section 230

Courts have developed a large body of law expansively applying Section 230 immunity. In 2012, one court noted it had located 300 reported decisions deciding the immunity. "All but a handful," the court noted, "find that the website is entitled to immunity."[16] Those seeking to circumvent the immunity have raised increasingly creative arguments, but with little success.

The year after Congress passed Section 230, the U.S. Court of Appeals for the Fourth Circuit became the first federal circuit to interpret the law, in the landmark decision *Zeran v. America Online, Inc.*, 129 F.3d 327 (1997). *Zeran* made clear that *Stratton Oakmont* really was gone, holding that Section 230 barred a defamation claim premised on AOL's failure to remove an allegedly libelous advertisement, even though the plaintiff repeatedly provided AOL notice about the content. The court reasoned that "Congress enacted § 230 to remove the disincentives to self-regulation created by the *Stratton Oakmont* decision."[17] "[I]n line with this purpose, § 230 forbids the imposition of publisher liability on a service provider for the exercise of its editorial and self-regulatory function."[18] The court rejected the plaintiff's argument that common-law principles of notice liability survived Section 230: "Liability upon notice would defeat the dual purposes advanced by § 230 of the CDA. Like the strict liability imposed by the *Stratton Oakmont* court, liability upon notice reinforces service providers' incentives to restrict speech and abstain from self-regulation."[19]

---

[13] Barton Swaim, *'The Twenty-Six Words That Created the Internet' Review: Protecting the Providers*, The Wall Street Journal, Aug. 19, 2019, available at https://www.wsj.com/articles/the-twenty-six-words-that-created-the-internet-review-protecting-the-providers-11566255518.

[14] 47 U.S.C. § 230(e)(3).

[15] 47 U.S.C. § 230(e)(1), (2).

[16] *Hill v. StubHub, Inc.*, 727 S.E.2d 550 (N.C. Ct. App. 2012).

[17] *Zeran v. America Online, Inc.*, 129 F.3d 327, 331 (1997).

[18] *Id.*

[19] *Id.* at 333.

After *Zeran*, every other federal circuit adopted a similarly broad interpretation.[20] Specific examples of broad interpretations include: the statute applies to distributors as well as publishers of speech, *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1104 (9th Cir. 2009) (distinction between publisher and distributor "has little to do with the meaning of the statutory language"); a provider is an "information content provider" of content only if it "contributes materially to the alleged illegality of the content," *Fair Housing Council v. Roommates.com*, 521 F.3d 1157, 1161-62 (9th Cir. 2008); merely "encouraging" unlawful content is insufficient to impose liability, *Jones v. Dirty World Entertainment Recordings LLC*, 755 F.3d 398, 403-06, 414 (6th Cir. 2014) ("an encouragement test would inflate the meaning of 'development' to the point of eclipsing the immunity from publisher-liability that Congress established"); and websites are not responsible for physical harm that occurs as a result of the perpetrator meeting the victim on the site, *Doe v. MySpace, Inc.*, 528 F.3d 413 (5th Cir. 2008) (rejecting minor's claim based on abuse she suffered after meeting a man on the MySpace website).

Reservations in the Courts

As technology companies became ever larger, however, courts became somewhat more skeptical of the breadth of Section 230 immunity, perhaps due to a perception that the internet no longer needed the same degree of protection Congress had granted it in 1996.

For example, in 2014, the Ninth Circuit held that Section 230 did not bar claims against a networking website based on a "failure to warn" theory, where two men posing as talent scouts had used information from a website to contact the victim, a model, and then drugged and raped her.[21] Most recently, earlier this month, the Ninth Circuit held that Snap, which operates an app that allows users to take and send snapshots, could not use Section 230 to bar claims brought by the parents of three children who died while using Snap's "Speed" filter, which measures the speed of a car in which a user is driving.[22] The plaintiffs argued that users expected (and Snap knew they expected) a reward for reaching more than 100 mph, and that that arrangement constituted a design defect in the app itself, subject to potential tort liability. According to the court, cases challenging the design of an app are not based on third-party content and thus survive Section 230.

Experienced judges at all levels have also criticized Section 230, albeit in dissents or separate opinions. In a sharp 2019 dissent, a Second Circuit judge stated that he would have held that Facebook was not immune from liability for facilitating the spread of terrorist messages, and welcomed the "healthy debate… in the legal academy and in the policy community about

[20] *See Jane Doe No. 1 v. Backpage.com, LLC*, 817 F.3d 12, 19 (1st Cir. 2016); *Ricci v. Teamsters Union Local 456*, 781 F.3d 25, 28 (2d Cir. 2015); *Jones v. Dirty World Entm't Recordings LLC,* 755 F.3d 398, 407 (6th Cir. 2014); *Johnson v. Arden*, 614 F.3d 785, 791 (8th Cir. 2010); *Doe v. MySpace, Inc.*, 528 F.3d 413, 418 (5th Cir. 2008); *Chi. Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc.,* 519 F.3d 666, 671 (7th Cir. 2008); *Lycos*, 478 F.3d at 419; *Almeida v. Amazon.com, Inc.*, 456 F.3d 1316, 1321 (11th Cir. 2006); *Green v. Am. Online*, 318 F.3d 465, 471 (3d Cir. 2003); *Ben Ezra, Weinstein, & Co. v. Am. Online Inc.*, 206 F.3d 980, 985 n.3 (10th Cir. 2000); *Zeran*, 129 F.3d at 331.

[21] *Doe v. Internet Brands, Inc.*, 767 F.3d 894 (9th Cir. 2014).

[22] *Lemmon v. Snap, Inc.*, 2021 WL 1743576 (9th Cir. May 4, 2021).

changing the scope of § 230."[23] And while the U.S. Supreme Court has not weighed in, Justice Clarence Thomas has twice criticized the universally broad application of Section 230 and made clear he would fundamentally alter the interpretation of the provision.[24]

Still, other than a few notable exceptions, Section 230 has remained largely intact in the courts.

Backlash in Congress

A similar change in attitude has developed in Congress. At first, "[f]ar from lowering the immunity bar, [Congress] ratcheted it up in 2010 by expanding the scope of section 230 immunity to preempt the enforcement of inconsistent foreign judgments.[25] But the tide has definitely turned.

Outrage over ads for sexual services, including trafficking of minors, led Congress to enact its first limits on Section 230's scope in 2018. That bill, known as FOSTA,[26] passed with overwhelming bipartisan support; only two senators voted "no."[27] FOSTA added a new exception to Section 230 for the enforcement of federal and state criminal or civil law relating to sex trafficking.[28] The act also made it a criminal offense to intentionally "promote or facilitate the prostitution of another person" online.[29]

President Trump signed FOSTA on April 11, 2018,[30] and the aftermath underscores how any effort to alter Section 230 may be fraught with complications and censorship.[31] Even before the President signed the law, Craigslist removed its entire personals section, citing risks posed to intermediaries "when third parties (users) misuse online personals unlawfully."[32] The self-censorship was widespread. Other sites with dating or escort-related content shut down entirely,

---

[23] *Force v. Facebook, Inc.*, 934 F.3d 53, 88 (2d Cir. 2019), *cert. denied*, 140 S. Ct. 2761, 206 L. Ed. 2d 936 (2020).

[24] *See Biden v. Knight First Amend. Inst. At Columbia Univ*., 141 S. Ct. 1220 (2021); *MalwareBytes, Inc. v. Enigma Software Group USA, LLC*, No. 19-1284 (Oct. 30, 2020) (denying petition for writ of certiorari).

[25] *Doe ex rel. Roe v. Backpage.com, LLC*, 104 F. Supp. 3d 149, 155-56 (D. Mass. 2015), *aff'd sub nom. Jane Doe No. 1 v. Backpage.com, LLC*, 817 F.3d 12 (1st Cir. 2016) (citing 28 U.S.C. § 4102(c)(1)).

[26] The House bill was the Allow States and Victims to Fight Online Sex Trafficking Act ("FOSTA"). An earlier Senate version was the Stop Enabling Sex Traffickers Act ("SESTA").

[27] Roll Call Vote, H.R. 1865, 115th Cong., 2nd Session (2018), available at https://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=115&session=2&vote=00060 (only Ron Wyden and Rand Paul voted against the bill).

[28] Allow States and Victims to Fight Online Sex Trafficking Act of 2017, H.R. 1865, 115th Cong. (2017), available at https://www.congress.gov/bill/115th-congress/house-bill/1865/text.

[29] *Id.*

[30] *Id.*

[31] *See* Aja Romano, *A new law intended to curb sex trafficking threatens the future of the internet as we know it*, Vox.com, Jul. 2, 2018, available at https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom.

[32] *Id.*

and Reddit banned multiple subreddits with sex-work-related content.[33] Companies like Google and Microsoft changed their policies and practices to limit adult content on their services.[34]

Challenges to FOSTA's constitutionality are pending. In *Woodhull Freedom Foundation v. United States*, a coalition of plaintiffs including human and sexual rights organizations, the Internet Archive, and individuals, challenged FOSTA under the First and Fifth Amendments. The court initially dismissed the case on standing grounds, but the D.C. Circuit reversed that decision, and the challenge is pending on cross-motions for summary judgment.[35] In *United States v. Martono*,[36] a trial court denied a criminal defendant's motion to dismiss charges of operating a website the government claimed facilitated prostitution, rejecting a constitutional challenge to FOSTA.

Since FOSTA, political efforts to reform or eliminate Section 230 have escalated, but the backlash is fueled by conflicting motivations.

Members of Congress from both parties have criticized Section 230, reminding tech companies that they are lucky to have it.[37] While they share a common distaste for Section 230, Democrats and Republicans disagree as to the nature of the problem: "Democrats say too much hate, election meddling, and misinformation get through, while Republicans claim their ideas and candidates are censored."[38]

Former President Trump frequently echoed these censorship concerns. In his last several months in office, he tweeted (or retweeted) calls to eliminate Section 230 upwards of 30 times.[39] At the end of his administration, he was so angry that he vetoed the National Defense Authorization Act

---

[33] *Id.*

[34] *Id.*; *see also* Tina Horn, *Sex-Worker Advocates Sue Over Internet 'Censorship' Law*, Rolling Stone, June 30, 2018, available at https://www.rollingstone.com/culture/culture-features/sex-worker-advocates-lawsuit-internet-censorship-sesta-fosta-666783/.

[35] *Woodhull Freedom Foundation v United States*, 948 F.3d 363 (D.C. Cir. 2020). *See Woodhull Freedom Foundation v United States*, No. 1:18-cv-1552 (D.D.C.).

[36] No. 3:20-CR-00274-N-1, 2021 WL 39584, at *1 (N.D. Tex. Jan. 5, 2021).

[37] Daisuke Wakabayashi, *Legal Shield for Websites Rattles Under Onslaught of Hate Speech*, The New York Times, Aug. 6, 2019, available at https://www.nytimes.com/2019/08/06/technology/section-230-hate-speech.html (In July 2019, "Senator Ted Cruz, Republican of Texas, said in a hearing about Google and censorship that the law was 'a subsidy, a perk'" for big tech that may need to be reconsidered. In an April [2019] interview, Speaker Nancy Pelosi of California called Section 230 a 'gift' to tech companies 'that could be removed.'"); *see also* Todd Shields and Ben Brody, *Washington's Knives Are Out for Big Tech's Social Media Shield*, Bloomberg, Aug. 11, 2020, available at https://www.bloomberg.com/news/articles/2020-08-11/section-230-is-hated-by-both-democrats-and-republicans-for-different-reasons.

[38] Todd Shields and Ben Brody, *Washington's Knives Are Out for Big Tech's Social Media Shield*, Bloomberg, Aug. 11, 2020, available at https://www.bloomberg.com/news/articles/2020-08-11/section-230-is-hated-by-both-democrats-and-republicans-for-different-reasons; *see also* Jessica Guynn, *Donald Trump and Joe Biden vs. Facebook and Twitter: Why Section 230 could get repealed in 2021,* USA Today, Jan. 4, 2021, available at https://www.usatoday.com/story/tech/2021/01/04/trump-biden-pelosi-section-230-repeal-facebook-twitter-google/4132529001/ ("Both parties threaten to narrow or repeal Section 230. Bottom line, they say, social media platforms should be held more accountable for how they police content. But their reasons are very different.").

[39] Trump Twitter Archive, available at https://www.thetrumparchive.com/?results=1&searchbox=%22230%22.

because it did not also repeal Section 230.[40] While President Biden has not afforded much public attention to Section 230 since taking office, early in his candidacy, in January 2020, he proclaimed that "Section 230 should be revoked immediately."[41]

Those questioning the value of Section 230 in its present form go beyond public officials. Large corporations have seized on the momentum against it in support of their own business-friendly goals. For instance, Marriott has lobbied against Section 230 because of the protection it provides to short-term rental services like Airbnb.[42] Meanwhile, companies such as Disney, Oracle, and IBM supported FOSTA.[43]

Proposals to Amend

These competing interests and views have led to numerous proposals.

Executive Proposals

The Trump Administration pushed to amend or clarify Section 230, and while those efforts have faltered with the presidential transition, they provide insight into how proposals to change the law from the right may proceed. In May 2020, President Trump issued an executive order related to "Preventing Online Censorship," which described Section 230's protections as "limited" and ordered the Federal Communications Commission (FCC) to propose regulations to "clarify" its application. In October, 2020, the FCC announced its intent to initiate a rulemaking to "interpret Section 230" and "clarify its meaning."[44] That announcement relied on Justice Thomas's view that courts have expanded Section 230 immunity "far beyond the actual text," and stated that online service providers have no right "to a special immunity denied to other media outlets, such as newspapers and broadcasters."[45] On May 14, however, President Biden revoked the Executive Order.[46]

---

[40] Timothy B. Lee, *House overrides Trump veto, defying demand to repeal Section 230*, Ars Technica, Dec. 28, 2020, available at https://arstechnica.com/tech-policy/2020/12/house-overrides-trump-veto-defying-demand-to-repeal-section-230/.

[41] Lauren Feiner, *Biden wants to get rid of law that shields companies like Facebook from liability for what their users post*, CNBC, Jan. 17, 2020, available at https://www.cnbc.com/2020/01/17/biden-wants-to-get-rid-of-techs-legal-shield-section-230.html.

[42] David McCabe, *IBM, Marriott and Mickey Mouse Take On Tech's Favorite Law*, The New York Times, Feb. 4, 2020, available at https://www.nytimes.com/2020/02/04/technology/section-230-lobby.html.

[43] *Id.*

[44] U.S. Fed. Communications Commission, *Statement Of Chairman Pai On Section 230*, Oct. 15, 2020, available at https://docs.fcc.gov/public/attachments/DOC-367567A1.pdf.

[45] *Id.* For a review of the FCC's authority to implement and interpret Section 230, see Congressional Research Service, *Section 230: An Overview*, Apr. 7, 2021, available at https://crsreports.congress.gov/product/pdf/R/R46751.

[46] Executive Order on the revocation of Certain Presidential Actions and Technical Amendment (May 14, 2021), available at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/14/executive-order-on-the-revocation-of-certain-presidential-actions-and-technical-amendment/.

The Department of Justice (DOJ) under the Trump Administration also conducted a review of Section 230 and proposed legislation that would substantially modify the statute.[47] DOJ's proposed legislation would constrain the scope of protection for decisions to remove content, broaden situations where a service provider is deemed responsible for creating content, and allow civil actions under anti-terrorism, child sex abuse, cyber-stalking, and antitrust laws.[48]

Other than repealing the Trump Administration Executive Order, President Biden's administration has taken no action with respect to Section 230, as other issues—such as the pandemic and economic recovery—have taken priority. Even so, the Biden Administration may pursue efforts to modify the law.[49]

Legislative Proposals

There is no shortage of congressional proposals to amend or eliminate Section 230. The 116th Congress (convened between January 3, 2019 and January 3, 2021) included 26 such bills.[50] The Congressional Research Service recently published a summary of those proposals.[51] Some prior Republican proposals have been reintroduced during the first few months of the current 117th Congress, although none have as of yet advanced out of committee or been the subject of significant debate. Among the proposals, a few have generated the most attention:

SAFE TECH Act

Perhaps the most high-profile effort to amend Section 230 is the "Safeguarding Against Fraud, Exploitation, Threats, Extremism, and Consumer Harms Act," or "SAFE TECH Act" (S.299), introduced in the Senate on February 5, 2021 by three Democrats.[52] If passed, the SAFE TECH Act would dramatically change the landscape of online liability under Section 230.

First, the Act would greatly limit the material protected by Section 230. It would exempt from protection content for which the provider pays or is paid. So websites could face liability for defamatory or misleading material in advertisements paid for by third parties, or in content for which the content provider pays. This amendment would fundamentally change the online advertising ecosystem, under which advertisers, not websites, bear the responsibility for their own content. Under the Act, websites would likely require liability insurance as a condition of hosting paid content. The SAFE TECH Act would also—like the Trump DOJ's proposal—

---

[47] U.S. Dept. of Justice, *Section 230 — Nurturing Innovation or Fostering Unaccountability?*, June 2020, available at https://www.justice.gov/file/1286331/download.

[48] U.S. Dept. of Justice, *Ramseyer Draft Legislative Reforms to Section 230 of the Communications Decency Act*, available at https://www.justice.gov/file/1319331/download.

[49] Rachel Lerman, *Social media liability law is likely to be reviewed under Biden*, The Washington Post, Jan. 18, 2021, available at https://www.washingtonpost.com/politics/2021/01/18/biden-section-230/.

[50] Congressional Research Service, *Section 230: An Overview*, Apr. 7, 2021, available at https://crsreports.congress.gov/product/pdf/R/R46751.

[51] *Id.*

[52] Safeguarding Against Fraud, Exploitation, Threats, Extremism, and Consumer Harms Act, S. 299, 117th Cong. (2021), available at https://www.warner.senate.gov/public/_cache/files/4/f/4fa9c9ba-2b34-4854-8c19-59a0a9676a31/66DECFBC0D6E6958C2520C3A6A69EAF6.safe-tech-act---final.pdf.

exempt from protection a raft of other laws, including those relating to civil rights, antitrust, stalking and harassment, international human rights, and wrongful death. Thus, Section 230 immunity would no longer be available for wide swaths of content, and the available protections would be narrower.

Second, the SAFE TECH Act would make it harder for providers to obtain the benefits of immunity by requiring courts to treat Section 230 as an affirmative defense. Today, courts frequently dismiss claims targeting third-party content at an early stage of the case, without requiring discovery. But the SAFE TECH Act would require the provider to plead and prove entitlement to protection from liability. This would increase the cost of defending claims and enable plaintiffs to file questionable lawsuits, hoping to extract a settlement. The burdens of such an approach would fall disproportionately on small providers, who may not have the resources to fight prolonged court battles.

Third, the Act would permit claims for injunctions against "material that is likely to cause irreparable harm." In other words, anytime someone believes that a posting causes them "irreparable harm," they can seek injunctive relief if a provider refuses to remove it. Again, this would have serious consequences—to evade Section 230 immunity, an individual need only request injunctive relief, even if the underlying content is lawful.

The SAFE TECH Act may be the most likely proposed amendment yet to gain traction. One of the bill's sponsors, Senator Mark Warner, has been meeting with President Biden's staff to discuss Section 230 and claims he expects to find a Republican co-sponsor.[53] At this point, however, the bill remains with the Committee on Commerce, Science, and Transportation.

Republican Proposals

Republican legislators continue to direct their anger over perceived censorship by online providers at Section 230 with proposals to dramatically reform or eliminate the law. For example, Rep. Louie Gohmert has proposed the "Abandoning Online Censorship Act" (H.R. 874), which simply states that "Section 230 … is repealed."[54] Rep. Jim Banks has proposed legislation (H.R. 2000) that would, according to the bill's summary, "clarify that [Section 230] does not prevent a provider or user of an interactive computer service from being treated as the distributor of information provided by another information content provider."[55]

More extensive proposals include the "Curbing Abuse and Saving Expression in Technology Act" or the "CASE-IT Act" (H.R. 285), which has two main parts. First, the CASE-IT Act would

[53] *Top Democrat speaks to Biden staff about key internet law*, Reuters, March 22, 2021, available at https://www.reuters.com/article/us-usa-democrat-tech/top-democrat-speaks-to-biden-staff-about-key-internet-law-idUSKBN2BE2EG.

[54] Abandoning Online Censorship Act, H.R. 874, 117th Cong. (2021), available at Text - H.R.874 - 117th Congress (2021-2022): AOC Act | Congress.gov | Library of Congress.

[55] H.R. 2000, 117th Cong. (2021), available at Text - H.R.2000 - 117th Congress (2021-2022): To amend section 230 of the Communications Act of 1934 to clarify that such section does not prevent a provider or user of an interactive computer service from being treated as the distributor of information provided by another information content provider, and for other purposes. | Congress.gov | Library of Congress.

strip immunity from a provider that "knowingly permits or facilitates an adult having contact through an interactive computer service of such provider with an individual that such adult knows or believes to be a minor, if such contact involves" sexual content.[56] Second, the bill would force large service providers to allow speech as if the provider were the government; and remove immunity from a provider that is "dominant in its market" and "makes content moderation decisions pursuant to policies or practices that are not reasonably consistent with the First Amendment to the Constitution."[57] The CASE-IT Act would also create a private right of action for those harmed by a provider's decision to "ban[] block[], down-rank[], demonetize[] in its advertising, or otherwise subject[] to similar adverse treatment the content of any information content provider… pursuant to policies or practices that are reasonably consistent with the First Amendment to the Constitution."[58]

Another proposal from Rep. Scott DesJarlais, entitled the "Protecting Constitutional Rights from Online Platform Censorship Act" (H.R. 83), would prohibit "any internet platform" from "restrict[ing] access to or the availability of protected material," defined as material "protected under the Constitution or otherwise protected under Federal, State, or local law."[59]

In the same vein, three Republicans introduced the "Limiting Section 230 Immunity to Good Samaritans Act" (H.R. 277) on January 12, 2021, which applies only to large tech companies.[60] The bill would mandate that providers implement terms of service with several specific components and provides that "intentionally selective enforcement" of the terms would cost a service provider its immunity under Section 230.[61]

Targeted Proposals

Other legislative proposals are more targeted. The bipartisan "See Something, Say Something Online Act of 2021" (S. 27), sponsored by Senators Joe Manchin and John Cornyn, would strip Section 230 immunity from any provider that "fails to report a known suspicious transmission"—meaning any user content that "commits, facilitates, incites, promotes, or otherwise assists the commission of a major crime."[62] A "major crime" includes crimes of violence, terrorism offenses, and serious drug offenses. The bill states that it is "not the intent of this Act to remove or strip all liability protection" provided by Section 230, but that "Congress

---

[56] Curbing Abuse and Saving Expression In Technology Act, H.R. 285, 117th Cong. (2021), available at Text - H.R.285 - 117th Congress (2021-2022): CASE-IT Act | Congress.gov | Library of Congress.

[57] *Id.*

[58] *Id.*

[59] Protecting Constitutional Rights from Online Platform Censorship Act, H.R. 83, 117th Cong. (2021), available at Text - H.R.83 - 117th Congress (2021-2022): Protecting Constitutional Rights from Online Platform Censorship Act | Congress.gov | Library of Congress.

[60] Limiting Section 230 Immunity to Good Samaritans Act, H.R. 277, 117th Cong. (2021), available at Text - H.R.277 - 117th Congress (2021-2022): Limiting Section 230 Immunity to Good Samaritans Act | Congress.gov | Library of Congress.

[61] *Id.*

[62] See Something, Say Something Online Act of 2021, S. 27, 117th Cong. (2021), available at Text - S.27 - 117th Congress (2021-2022): See Something, Say Something Online Act of 2021 | Congress.gov | Library of Congress.

intends to look at removing liability protections" if online providers "fail to exercise due care" in implementing the bill's reporting requirements.[63] The bill would substantially affect how providers operate. Providers would be torn between turning a blind eye to avoid learning of any potential criminal activity on their platforms, or closely surveilling user activity to ensure no "major crime" falls through the cracks.

Another narrower proposal is the bipartisan "Protecting Local Authority and Neighborhoods Act" or the "PLAN Act" (H.R. 1107), which would make clear that Section 230 does not provide immunity for providers who are on notice that their platforms are being used to facilitate unlawful rentals.[64] In doing so, the bill would prevent short-term online rental sites such as Airbnb from using Section 230 as a defense against local restrictions on short-term rentals.

First Amendment Concerns

Putting aside the significant political hurdles, many proposals are also likely to face First Amendment challenges.[65] Concerns about how to square free speech with what some characterize as the web's Wild West tendencies are not new: the Supreme Court as early as 1997 confronted how to balance the protection of minors from sexual exploitation with the internet's potential for creating "vast democratic forums."[66] Most recently, the Supreme Court in 2017 deemed the internet, and in particular social media, "the most important place" for the modern day "exchange of views."[67] And last year, in a decision that was ultimately vacated for mootness, the Second Circuit found that then-President Donald Trump's public Twitter feed was a government-run public forum subject to First Amendment protections.[68]

But Congress cannot treat internet service providers as though they were the government for purposes of content moderation. Editorial discretion about what to publish and what not to publish are at the very core of private entities' First Amendment rights—even though the First Amendment bans the government from making those very same types of decisions. This concern would arise, for example, with H.R. 277's ban on selective enforcement, or H.R. 287's requirement that providers not engage in "censorship." Providers have First Amendment rights, and, citing cases like *Miami Herald Pub. Co. v. Tornillo*,[69] would likely argue that their decisions about what *not* to publish are constitutionally protected to the same extent as their decisions about what to allow—just as the Supreme Court held that the newspaper in *Tornillo* had a First Amendment right to decide which editorials to include and exclude. In short, Congress cannot

---

[63] Text - S.27 - 117th Congress (2021-2022): See Something, Say Something Online Act of 2021 | Congress.gov | Library of Congress

[64] Protecting Local Authority and Neighborhoods Act, H.R. 1107, 117th Cong. (2021), available at Text - H.R.1107 - 117th Congress (2021-2022): PLAN Act | Congress.gov | Library of Congress.

[65] *See, e.g.*, Congressional Research Service, *Section 230: An Overview*, Apr. 7, 2021, available at https://crsreports.congress.gov/product/pdf/R/R46751 (evaluating First Amendment issues with various reform proposals).

[66] *See Reno v. ACLU*, 521 U.S. 844, 868 (1997).

[67] *Packingham v. North Carolina*, 137 S. Ct. 1730, 1735 (2017).

[68] *See Knight First Amend. Inst. at Columbia Univ. v. Trump*, 953 F.3d 216, 220 (2d Cir. 2020).

[69] 418 U.S. 241 (1974).

force providers to retain user content just because that content is itself protected speech (of the providers' users) under the First Amendment.[70]

A common problem with the proposals is their treatment of Section 230 immunity as a matter of legislative grace, one that Congress may grant, modify, or withdraw at will. However, without regard to legislative preferences, the First Amendment has long extended protection to decisions by speech intermediaries. Well before the internet, the Supreme Court repeatedly recognized that laws threatening liability on those who provide a forum for speech pose special threats to the rights of speakers and readers who depend on those services. In *Smith v. California*,[71] for example, the Court struck down a law holding booksellers strictly liable for obscene books on their shelves because the law would in effect compel self-censorship by the bookstore. The problem, the court noted, was "[t]he bookseller's limitation in the amount of reading material with which he could familiarize himself, and his timidity in the face of his absolute criminal liability, thus would tend to restrict the public's access to forms of the printed word which the State could not constitutionally suppress directly."[72] For similar reasons, the Court rejected Rhode Island's bookseller liability laws in *Bantam Books v. Sullivan,*[73] and later upheld cable programmers' First Amendment challenge to laws requiring cable operators to segregate and block patently offensive sexual content.[74]

The concerns expressed in *Smith*, *Bantam Books*, and *Denver Area* are particularly acute in the internet context due to the volume of speech. Thus, in *Center for Democracy & Technology v. Pappert*,[75] the court struck down a Pennsylvania statute requiring ISPs to block child pornography upon notice, which had led ISPs to block lawful content as well. The court reasoned that even though the law, "on its face, does not burden protected speech[,] … the action taken by private actors to comply with the Act has blocked a significant amount of speech protected by the First Amendment." *Id.* at 652 (applying *U.S. v. Playboy Ent. Grp., Inc.*, 529 U.S. 803 (2000)). *See also Cubby v. Compuserve*, 776 F. Supp. 135, 139 (S.D.N.Y 1991)) (expressing concerns "deeply rooted in First Amendment" that intermediary not be treated as a publisher in defamation case).

Section 230 incorporated First Amendment values to promote free online expression, free intermediaries from threats of liability for hosting third-party speech, and encourage websites to

---

[70] A number of lower courts have upheld First Amendment protections for online editorial decisions. *See, e.g., e-ventures Worldwide, LLC v. Google, Inc*., 2017 WL 2210029, at *4 (M.D. Fla. Feb. 8, 2017) (exercise of online editorial discretion is "the same as decisions by a newspaper editor regarding which content to publish, which article belongs on the front page, and which article is unworthy of publication"); *La'Tiejira v. Facebook, Inc.*, 272 F. Supp. 3d 981, 991-22 (S.D. Tex. 2017); *Jian Zhang v. Baidu.com Inc.*, 10 F. Supp. 3d 433, 438-39 (S.D.N.Y. 2014) (online platforms "are engaging in fully protected First Amendment expression—[t]he presentation of an edited compilation of speech generated by other persons"); *Langdon v. Google, Inc.*, 474 F. Supp. 2d 622, 629-30 (D. Del. 2007) (First Amendment protects decisions by intermediaries).

[71] 361 U.S. 147 (1959).

[72] *Id.* at 153-54.

[73] 372 U.S. 58 (1963).

[74] *Denver Area Educ. Telecom. Consortium v. FCC*, 518 U.S. 727 (1996).

[75] 337 F. Supp. 2d 606, 649-650 (E.D. Pa. 2004).

make editorial judgments without risking liability.[76] As the Fourth Circuit explained in *Zeran*, service providers' inability to screen each of the millions of posts requires them either to make "an on-the-spot editorial decision whether to risk liability by allowing the continued publication" or yield to the "natural incentive simply to remove messages upon notification, whether the contents were [unlawful] or not[.]"[77] The *Zeran* court understated just how daunting a task this has become. By 2019, more than 500 hours of third-party content were being uploaded to YouTube *per minute*. That works out to 30,000 hours of new content per hour, and 720,000 hours of new content per day (equivalent to 82.2 years).[78]

Modifying Section 230 might change legislative *recognition* of this constitutional imperative, but it would not cancel the underlying First Amendment concerns. If the federal government had, for example, adopted a law to preserve First Amendment values online by barring civil claims against online platforms that host indecent expression, Congress might later decide to eliminate that legislative protection—but doing so would not diminish the First Amendment bar to bringing such claims.[79] As the Supreme Court has stressed, "[m]ere legislative preferences or beliefs respecting matters of public convenience" may not "diminishe[]… rights… vital to the maintenance of democratic institutions."[80] Accordingly, proposals designed to increase the threat of liability for online intermediaries' moderation decisions inevitably raise significant constitutional questions.

Congress cannot avoid this problem by crafting bills to provide "incentives" that would allow platforms to "earn" Section 230 immunity, or by attempting to regulate moderation policies or decisions as "trade regulations." Even if Section 230 immunity could be characterized as a mere "benefit," government may not withhold it based on a platform's relinquishment of its ability to set its own rules. The Supreme Court has long held that the government may not deny a benefit to a person on a basis that infringes his constitutionally protected freedom of speech even if he has no entitlement to that benefit.[81] Nor are constitutional barriers to regulating content selection ameliorated by framing the law as trade regulation. *Cf.*, *Prager Univ. v. Google*, 951 F.3d 991, 1000 (9th Cir. 2020) (rejecting Lanham Act claim based on moderation decisions); *FreedomWatch, Inc. v. Google*, 816 Fed. Appx. 497 (D.C. Cir. 2020), *cert. denied*, 2021 WL 1240927 (2021) (rejecting Sherman Act claim against YouTube for allegedly suppressing conservative political views).

Additionally, some current proposals could also encounter problems because they draw distinctions on the basis of the content of speech. If the proposed reforms sought, for example, to

---

[76] *Google v. Hood*, 822 F.3d 212, 220 (5th Cir. 2016).

[77] 129 F.3d. at 333.

[78] *See, e.g.*, James Hale, tubefilter, May 7, 2019, available at https://www.tubefilter.com/2019/05/07/number-hours-video-uploaded-to-youtube-per-minute/; H. Tankovska, *Hours of video uploaded to YouTube every minute as of May 2019*, statista, Jan. 26, 2021, available at https://www.statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute/.

[79] *Reno*, 521 U.S. at 871-874.

[80] *Schneider v. Town of Irvington*, 308 U.S. 147, 161, 162 (1939).

[81] *Speiser v. Randall*, 357 U.S. 513, 526 (1958); *Agency for Intern. Development v. Alliance for Open Society Int'l.*, 133 S.Ct. 2321 (2013).

ban any form of political speech, that would be a content-based restriction subject to strict scrutiny. And if a reform aimed to ensure platforms do not sideline a specific kind of political speech, such as conservative speech, opponents could argue that the bill seeks to impose viewpoint discrimination, which courts almost never find constitutional.

Other bills appear to attempt to limit restrictions on unprotected speech only, but at least at this juncture, have almost certainly painted with too broad a brush. The "See Something Say Something Act," for example, would require providers to report speech that "promotes….the commission of a major crime." But the majority of speech that promotes commission of a crime is in fact protected, with an exception only for speech advocating that a crime be committed *imminently* to lose First Amendment protection.[82] Similarly, reform aimed at prohibiting hate speech would likely run afoul of current First Amendment law, which contains no such exception.

The knowledge or intent requirements of some proposals could also present First Amendment issues. S. 27, for instance, requires providers to report "suspicious transmissions" of which they know or reasonably should know.[83] But, as noted above, the First Amendment generally precludes holding a publisher or distributor liable for a third party's speech without specific knowledge that the speech was unlawful.[84] Under this test, the CASE-IT Act may be problematic because it would strip protection from providers who "knowingly" permit an adult to have contact with a person "that such adult knows or believes to be a minor"—thus potentially charging the provider with responsibility to know what its user "knows or believes" about another person's age.

Basing liability or takedown requirements on "knowledge" of problematic content derived from complaints is also problematic. Courts have been particularly wary of the "heckler's veto," whereby a law empowers others to censor speech by simply complaining to the intermediary about it (and thereby providing "notice").[85] They recognize that intermediaries will often respond to complaints by simply deleting the speech complained of or by eliminating the platform, rather than expend the resources to investigate the complaint's merits. *Id.* As the Supreme Court observed, the concern for censorship is magnified with respect to online intermediaries as they may have to deal with thousands and thousands of complaints every day. Regimes that require website operators to remove content based on such knowledge "confer broad powers of censorship, in the form of a 'heckler's veto,' upon any opponent of indecent speech."[86]

[82] *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969).

[83] See Something, Say Something Online Act of 2021, S. 27, 117th Cong. (2021), available at Text - S.27 - 117th Congress (2021-2022): See Something, Say Something Online Act of 2021 | Congress.gov | Library of Congress.

[84] *See, e.g., Smith*, 361 U.S. at 153-154.

[85] *See Reno*, 521 U.S. at 880.

[86] *Id.* at 880.

Conclusion

Members of Congress continue to introduce proposals to reform or repeal Section 230. Broad bipartisan dissatisfaction with Section 230 ensures that we have not heard the end of the story. But the fact that the parties have fundamentally different concerns significantly decreases the chance of any actual reform. And indeed, other than FOSTA, no major limits to Section 230 have been enacted. If recent efforts at reform provide any lesson, it is that no reform will be as simple as it seems. Online speech has developed largely unrestricted for 25 years, and changes—no matter how well intended—will certainly lead to litigation, and likely unintended consequences (which will then invite further reform).