Communications Lawyer
Publication of the Forum on Communications Law
American Bar Association
Volume 33, Number 4, Spring/Summer 2018
THE JOURNAL OF MEDIA, INFORMATION, AND COMMUNICATIONS LAW

In this issue

The Differing US and EU Regulatory Responses to Rise in Algorithmic Profiling

BY PHILIP N. YANNELLA

The online world is increasingly shaped by forces beyond our control. Algorithmic processing agents are used by a wide range of web publishers, online retailers, and social media companies to determine the kinds of stories that are featured to online readers, the advertisements that are targeted to online shoppers, and the search results they see, to name just a few of the ways in which these hidden programs predict the shape and content of our online experience. Beyond the world of advertising, algorithms are used to make decisions about insurance premiums, healthcare, education, housing, and employment.

Recently, information scientists, ethicists, and legal scholars have begun to identify the potential negative effects of algorithmic agents—such as the potential to enable discriminatory decision making—but there is little consensus on how to regulate the increasing use of algorithms. The marketplace has not yet settled on a supply-demand solution, and self-auditing and independent auditing of algorithms have proven to be technologically challenging, hampering the development of self-regulatory codes.

The other potential mechanism for regulating algorithms is through legal means. This article will explore the very different approaches emerging in the two largest legal systems to have addressed these issues: those in the United States and the European Union.

Potential Negative Effects of Online Algorithmic Agents

Many people believe that algorithmic processing tools are harmless robots that rely on objective criteria to render fact-based predictions about consumer likes and behavior. As information science grows as a discipline, however, scientists are increasingly recognizing that algorithm processing agents are not necessarily objective and can be used for discriminatory purposes or have the effect of magnifying discriminatory attitudes of online users.

The *New York Times* recently reported on a Carnegie Mellon University study that found that Google's online advertising system showed an ad for high-income jobs to men much more often than it showed the ad to women.[1] Similarly, Harvard University researchers determined that advertisements for arrest records were more likely to be displayed in searches for distinctively black names or a historically black fraternity.[2] The *New York Times* also reported on a University of Washington finding that a Google Images search for "CEO" produced 11 percent women, even

Continued on 19

Mr. Yannella is the co-chair of the privacy and data security group at Ballard Spahr LLP. He focuses his practice on providing clients with 360-degree legal advice on the collection, storage, use, and transfer of digital information.

FROM THE CHAIR

Honoring John Borger—A Champion of the First Amendment

INTRODUCTORY REMARKS BY STEVEN D. ZANSBERG

At the Forum's 2018 Annual Conference, our friend and colleague John Borger was presented with the Champion of the First Amendment award for all of his outstanding achievements throughout his career as a guardian of the First Amendment. Presented below is Steve Zansberg's glowing introduction of John, followed by John's inspiring acceptance speech.

It is my honor and privilege to present the ABA Forum's Champion of the First Amendment award to our colleague and friend John Borger.

I am not going to attempt to chronicle the incredible career of John Borger. Instead, we have provided you all with a copy of his résumé as it appeared on the Faegre Baker Daniels website at the time of his retirement last year. I commend that to you, so you can see and appreciate both the depth and breadth of John's professional experience.

John is well known to, and much beloved by, many in this room. In fact, when John was nominated to receive this award, some of the newer members of the Forum's Governing Committee weren't aware that this award even existed, or what it was for. So, I explained that this award is not something the Forum gives out with any frequency or regularity—indeed, we have bestowed it only twice previously—to Dick Winfield and Jim Goodale—both of whom are "Founding Fathers" of this community of ours, a/k/a the organized "media law bar." The award is designed to honor those who not only ("merely") devoted their entire careers to fighting to protect freedom of speech and of the press, but also, and *especially*, those who have made sustained and significant contributions to the development of this bar (our community). When I finished describing the criteria for the award, the Governing Committee, *without further discussion*, voted *unanimously* to bestow it on John.

Prior to becoming a lawyer, John was a journalist—a reporter and then editor-in-chief, at his college paper, *The Michigan State News*, where he met his fellow budding journalist and later wife (now of forty-three years), Judy. Thus, it was at the early stage of his professional life that John developed two of his three life passions: first and foremost, his family, and second, the fight for freedom of the press.

I had the good fortune to spend the first ten years of my legal career working with John, at Faegre & Benson, and to benefit from his wisdom, counsel, mentoring, and warm friendship. John's knowledge of First Amendment law is so encyclopedic that during the annual First Amendment/Journalism Jeopardy program, that George Freeman created and emcee'd for so many years at this conference, people entering the lunchroom would jockey for a seat at John's table in the hopes of sharing the victory.

As many in this room can personally attest, John is, and has always been, incredibly giving of his time and energies—both to his colleagues and

Communications Lawyer (ISSN: 0737-N7622) is published four times a year by the Forum on Communications Law of the American Bar Association, 321 North Clark St., Chicago, IL 60654-7598. POSTMASTER: Please send address corrections to ABA Service Center, 321 North Clark St., Chicago, IL 60654-7598. The opinions expressed in the articles presented in ***Communications Lawyer*** are those of the authors and shall not be construed to represent the policies of the American Bar Association or the Forum on Communications Law.

peers, and to organizations he joins, including at this Forum, and the Torts, Trial and Insurance Practice Section, where he edited its annual Survey of Media Law for more than a decade.

John is a consummate wordsmith. Leita Walker tells me he once corrected her for misusing the word "decimate" because it means "to smite one in ten of a population," not, as many of us commonly misunderstand it, to mean to utterly destroy.

John also has a dry sense of humor. He loves to dispense groan-inducing puns. True to form, one of his many law review articles, about misuse of the tort of trespass against the press, was entitled "New *Whines* in Old Bottles: Taking Newsgathering Torts Off the Food Lion Shelf."

Not everyone knows this, but John also has a *third* passion—you might say obsession—he is a fan (which is short for "fanatic") of superheroes of the DC Comics and Marvel vintage. In 2008, when John and Judy moved out of their big old house into their smaller downtown condo, John donated his personal collection of over 40,000 comic books (valued at well over $100,000, with several "issue no. 1"s in popular series) to the University of Minnesota. The John Philip Borger Comic Books Collection, each volume fully catalogued, now resides in that university library's permanent repository.

So, in addition to presenting him with yet another ornament to adorn an already crowded trophy wall, we are also presenting him this t-shirt, which recognizes John as ***Superman* of the First Amendment.**

Of course, his family—including Judy; their three kids, Nick, Chris, and Jenny (all of whom are with us today); their significant others; and John and Judy's six grandchildren—also take him as their hero, so long as he doesn't take to wearing a cape. ("No capes!")

I will now read for you what the plaque says before inviting John to come up on stage and share a few words. It reads:

> For more than four decades of providing wise counsel to the Minneapolis Star Tribune, and numerous other members of the press; for passionately and zealously fighting to hold public officials and institutions accountable through transparency; for helping to organize and lead the "media bar," and for other countless and tireless efforts in support of Freedom of the Press, the ABA Forum on Communications Law hereby honors
>
> JOHN BORGER
>
> as a true "Champion of the First Amendment"

(Editors' Note: Steve's introduction was followed by a thunderous and lengthy standing ovation.)

Champion of Freedom Remarks by John Borger:

Thank you for that generous introduction, Steve. And thank you, Carolyn and members of the Governing Committee and the entire Forum, for this award. It is special because it comes from all of you. The media bar is a community of passionate, intelligent, inquisitive, and collegial lawyers. We are privileged to represent clients who, at their best, are guardians of democracy and persistent seekers of truth in service of justice.

To have a career full of such clients and colleagues has been a blessing far beyond anything I could have predicted in college and law school. Oh, what a time it was. A time of innocence. A time of confidences and possibilities and determination to make the world a better place. Yet also a time of social unrest, and conflicts between young and old, black and white. Young soldiers died in foreign lands, fighting an unpopular war. At home, authorities arrested, gassed, even shot and killed protestors. A presidential election was marred by deep divisions within the Democratic Party and by a Republican candidate engaged in clandestine communications with a foreign power. A president's name became an epithet. A special prosecutor investigated presidential misconduct. An administration engaged in systematic assaults on the press. Rising to the occasion, *The New York Times* and the *Washington Post*, like the Beatles and the Beach Boys, challenged each other to ever-greater achievements. A terrific movie about journalism inspired young reporters and young lawyers. My, the times they've been a-changin'.

One change was a long time comin', but it's helped us all to be able to carry on. That is the growth of the organized media bar. The creation and development of that bar has not been an accident or a coincidence. It's the result of hard work by

- Leaders like First Amendment scholars Thomas Emerson and Don Gillmor.
- Leaders like Floyd Abrams, Dick Winfield, Jim Goodale, Victor Kovner, Bob Sack, Cam DeVore, and Conrad Shumadine, whose PLI conferences provided a platform for this practice to meet nationally and to establish lasting personal relationships.
- Leaders like Larry Worrall and Chad Milton, who understood that insuring news organizations is not the same as insuring cars.
- Like Jack Landau, Jane Kirtley, Lucy Dalglish, and Bruce Brown, at the Reporters Committee for Freedom of the Press.
- Like Henry Kaufman and Sandy Baron and George Freeman, at the Media Law Resource Center.
- And like Barbara Wall, Lee Levine, Kelli Sager, and George Freeman, who launched and led this very conference 20-some years ago.

We owe them all an enormous debt.

I owe my center and my sanity to the blessings in my personal life: Judy, my wife, my rock, and my sun and stars; my remarkable children Jen and Chris and Nick, whose presence here today makes this truly the room where it happens; and six amazing grandchildren, who blow my world away. With a nod to those grandchildren, I offer this piece of pseudo-Seussian verse: I loved what I did, and I did what I loved; free speech is a First Right, when push comes to shove.

I have carried a torch for the First Amendment for more than 50 years. I hope I lit a few candles along the way. The First Amendment torch now burns with you, and you, and you. Hold it high. The road goes ever on and on. Many important battles lie ahead. But look around the room and know this: You will never, ever, walk alone. ■

You May Be Able to Outsource Privacy and Cybersecurity Functions, but You Can't Outsource the Risk of Liability

BY EVE REED AND KATHLEEN SCOTT

Communications companies today face a wide and seemingly ever-increasing variety of privacy and cybersecurity obligations. Some of these legal requirements apply broadly across industries and activities, including data security and privacy requirements enforced by the Federal Trade Commission (FTC), while some of them apply only to specific industry sectors, such as those under the Cable Privacy Act or the Satellite Privacy Act. And some obligations apply to specific types of data, like those under the Children's Online Privacy Protection Act (COPPA), while others apply to particular activities, like those under the Telephone Consumer Protection Act (TCPA) or the CAN-SPAM Act. As a result, a single company can find itself juggling multiple regimes from a variety of federal agencies. Taking into account additional state regulation and oversight, it is clear that privacy and cybersecurity compliance can quite quickly become very complicated.

To manage these obligations and continue to utilize modern-day technology to provide better products and services, many companies turn to third-party vendors to perform a variety of tasks, ranging from managing data to directly contacting consumers. This practice has many potential benefits, including allowing small – and medium-sized companies to take advantage of sophisticated privacy and cyber tools that they may not possess internally but that vendors may allow them to utilize. However, companies should be careful not to ignore legal and regulatory obligations simply because they have hired a third party to perform the task. Outsourcing obligations can make a lot of sense; however, doing so does not absolve a company from legal responsibility. It is therefore critical that companies utilizing third-party vendors understand—and carefully oversee and direct—the actions of those third-party vendors.

The Complex Compliance Landscape

The privacy and cyber legal landscape is complex and continuously becoming more complicated. Below are nonexhaustive examples of regimes—at both the federal and state levels—that a communications company *may* face.

In general, all companies need to be aware of the FTC's involvement in privacy and data security. Section 5 of the FTC Act prohibits "unfair or deceptive practices in the marketplace."[1] The FTC uses this authority as one of its tools to protect consumer privacy and data security; the agency boasts having "brought hundreds of privacy and data security cases protecting billions of consumers."[2] The FTC's jurisdiction in this area is not limitless; for example, the FTC Act bars the FTC from exercising its authority against "common carriers subject to the Acts to regulate commerce," including the "Communications Act of 1934."[3] The precise scope of this "common carrier exception" has been debated by the courts, with conflicting interpretations emerging[4] and a final resolution increasingly important given the ongoing dispute over net neutrality.[5] Regardless, the FTC's responsibilities for privacy and cybersecurity do extend to many communications companies.

There are also privacy and cyber obligations that are specific to the communications sector or specific segments of that sector. For example, the Cable Privacy Act[6] and the Satellite Privacy Act[7] impose duties on cable and satellite providers to protect the personally identifiable information (PII) of subscribers, including notice and consent requirements,[8] duties regarding a subscriber's ability to access and correct such data,[9] and data retention and destruction obligations.[10] There are also specific privacy rules for telecommunications carriers dealing with customer proprietary network information (CPNI), such as a telephone subscriber's call detail records.[11] Under the CPNI rules adopted by the Federal Communications Commission (FCC), a telecommunications carrier, among other things, must notify its customers of its privacy policies and material changes to such policies[12] and comply with consent requirements prior to using, disclosing, or permitting access to CPNI under certain circumstances.[13] The FCC, under more general authority, also has brought enforcement actions against regulated companies for allegedly failing to protect sensitive personal information.[14]

Additionally, companies may face privacy and data security obligations based on the type of information they are dealing with. For example, if a company is an "operator[] of commercial websites and online services (including mobile apps) directed to children under 13 that collect, use, or disclose personal information from children, [or an] operator[] of general audience websites or online services with actual knowledge that

Eve Reed is a partner, and Kathleen Scott is an associate, in the telecom, media, and technology practice at Wiley Rein LLP.

[it is] collecting, using, or disclosing personal information from children under 13,"[15] the company must comply with COPPA. COPPA was designed to "place parents in control over what information is collected from their young children online," and its rules, implemented by the FTC, create several compliance obligations, including an obligation to "[m]aintain the confidentiality, security, and integrity of information they collect from children, including by taking reasonable steps to release such information only to parties capable of maintaining its confidentiality and security."[16] The FTC also has special guidance for other specific types of data—for example, certain geolocation data.[17]

A company also can become subject to privacy regimes by taking specific actions. For example, the Telephone Consumer Protection Act (TCPA), which is implemented by the FCC, establishes certain privacy protections for consumers when companies use automated calling equipment to contact them.[18] Based on the circumstances of the calls and the specific equipment used, companies often are required to obtain consent—the precise form of which is dictated by FCC rules—before placing automated calls.[19] Further, the FTC's Telemarketing Sales Rule[20] and the FCC's TCPA rules[21] impose specific obligations upon entities engaging in telemarketing activities. And companies must consider the CAN-SPAM Act, which is primarily implemented by the FTC, when communicating with consumers via email.[22]

States are active in the privacy and cyber arenas as well, which requires companies to pay attention to a wide variety of state laws and regulations. For example, several states have adopted cybersecurity standards for commercial entities that store, collect, process, or maintain certain data.[23] California, as an example, mandates that "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[24] Massachusetts, as another example, has established detailed requirements for companies to "develop, implement, and maintain a comprehensive information security program."[25] States also regulate privacy—for example, California and Delaware both have enacted laws that require companies to post privacy policies online and dictate the contents of those privacy policies.[26]

Communications companies must consider all of these various regimes—and more—to ensure that they have an adequate approach to cyber and privacy. Failure to do so could expose a company to legal and regulatory risk and, in this era, also could expose a company to negative attention from consumers, who care increasingly about the privacy and security of their personal information.

Third-Party Vendor Issues

Given the complex regulatory landscape, many companies turn to third-party vendors to manage data, reach out to customers, or otherwise deal with privacy and cybersecurity issues. This practice is often the right move for companies that seek to leverage sophisticated tools and subject-matter expertise possessed by specialized vendors. However, it is important to proceed with extreme caution in this area: Outsourcing cybersecurity and privacy obligations does not absolve a company from its legal responsibilities.

Several regimes discussed above (and, in some cases, related guidance) explicitly address third-party vendor scenarios. As the below examples illustrate, it is clear that companies cannot avoid privacy and cyber obligations by simply contracting with a third party:

- **COPPA:** In its guidance to companies subject to the COPPA regime, the FTC states as follows: "Before sharing information with [third-party providers], you should determine what the service providers' or third parties' data practices are for maintaining the confidentiality and security of the data and preventing unauthorized access to or use of the information. Your expectations for the treatment of the data should be expressly addressed in any contracts that you have with service providers or third parties. In addition, you must use reasonable means, such as periodic monitoring, to confirm that any service providers or third parties with which you share children's personal information maintain the confidentiality and security of that information."[27]
- **TCPA:** The FCC's TCPA regulations contemplate a scenario where a "telemarketer"—the "person or entity that initiates a [telemarketing] telephone call or message"—is different than a "seller"—the "person or entity on whose behalf a [telemarketing] telephone call or message is initiated."[28] Both have obligations under the rules.[29] The FCC highlighted this distinction in 2013 guidance, which explained that a company may be "held vicariously liable under federal common law principles of agency for violations of [the TCPA] that are committed by third-party telemarketers."[30] The Commission also has made clear that a company cannot simply avoid TCPA liability by outsourcing its calling: "[A]llowing the seller to avoid potential liability by outsourcing its telemarketing activities to unsupervised third parties would leave consumers in many cases without an effective remedy for telemarketing intrusions. . . . Even where third-party telemarketers are identifiable, solvent, and amenable to judgment, limiting liability to the telemarketer that physically places the call would make enforcement in many cases substantially more expensive and less efficient, since consumers (or law enforcement agencies) would be required to sue each marketer separately in order to obtain effective relief."[31] As is the case with many TCPA issues, the question of liability for the actions of third-party vendors has played out in the courts as well. In *Hartley-Culp v. Green Tree Servicing, LLC*,

for example, a federal district court held that "the TCPA can impose liability directly or vicariously upon any person or entity on whose behalf a third party places a call in violation of [the TCPA]."[32]

- **TSR:** As discussed above, certain common carriers—such as telecom common carriers—enjoy an exception from FTC authority under the FTC Act.[33] However, "the Commission has . . . made it very clear that the exemption enjoyed by [common carriers] does not extend to any third-party telemarketers who may make or receive calls on behalf of those exempt entities."[34]
- **CAN-SPAM:** A key principle of CAN-SPAM that the FTC reiterates to companies is to "[m]onitor what others are doing on your behalf. The law makes clear that even if you hire another company to handle your email marketing, you can't contract away your legal responsibility to comply with the law. Both the company whose product is promoted in the message and the company that actually sends the message may be held legally responsible."[35]
- **California State Law:** California's cybersecurity law requires that a company working with a "nonaffiliated third party" must contract with that third party to ensure that the third party "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[36]

What is also clear is that third-party vendors are not perfect and that they can face privacy and cyber issues regardless of their level of expertise and sophistication. Data breaches provide a good example. Indeed, one study indicated that a full 63% of data breaches can be attributed to third-party vendors.[37] Recent headlines reiterate this point. In one incident, a healthcare vendor that provided software and electronic health record services was hacked, impacting over 300,000 patients from the over 15,000 healthcare-provider clients of the vendor.[38] In another incident, a vendor that was used by major retailers including CVS and Costco to manage online photo centers was hacked, exposing customer records.[39] While litigation in this instance was focused on the vendor, the vendor's clients (here, major retailers) still faced reputational harm.

Third-party vendors are not perfect and can face privacy and cyber issues regardless of their level of expertise and sophistication.

Tips for Responsible Outsourcing

Given the complexity of the privacy and cyber landscape and the real risks faced by companies, even when they engage third-party vendors, it is critical to remain diligent in managing third parties. Companies should consider the following top five tips to manage these risks:

- **Do the work up front to assess your vendor's privacy and security posture**. Not all third-party vendors are created equally, and some have more robust practices than others. Before engaging a vendor, do the necessary due diligence to determine where your proposed vendor falls on the scale. It may be helpful to have a general questionnaire that you use across all vendors so that you can easily compare and contrast. However, be careful not to overgeneralize in this phase. Due diligence should be tailored to your specific objectives, so do not be restricted by any questionnaire that you may develop.
- **Include cyber and privacy obligations in your contract.** Make your vendor's privacy and security obligations clear in your contract. Some regimes—for example, the California cyber regime discussed above—explicitly require this. Others do not, but it is generally a best practice to do so. Here, as in the due diligence phase, tailoring the agreement to fit your specific business objectives is critical. There will be no one-size-fits-all contract. However, there are certain obligations that generally should be included: (1) require that vendors notify you of any problem or incident that arises; (2) require that vendors update their policies regularly to reflect changing laws and technologies; (3) ensure that you have the right to regularly audit your vendor; and (4) ensure that you have the right to terminate the relationship if necessary. In addition, it is a good idea to try to build in flexibility to account for changes in the law by, for example, defining a particular statutory or regulatory obligation to include amendments, supplements, and guidance, as well as replacement statutes or regulations.
- **Consider an indemnification clause, but realize that is not a silver bullet.** In addition to making clear who is responsible for what in the contract, companies can consider including an indemnification clause to channel any liability back to the vendor. But an indemnification clause should not be viewed as a "get-out-of-jail-free" card for companies. Even with a robust indemnification clause, some vendors will not have the money to cover class action verdicts or settlements, which can be astronomical in certain of the settings discussed above. For example, in 2017, DISH was hit with $61 million in damages in a TCPA class action (which in part involved calls made by a third-party vendor)[40] and another $280 million in damages in an action brought by the FTC and several states.[41] These amounts are so large as to create a question whether any vendor—even a very reputable one—could

satisfy them. What is more, indemnification clauses will not protect companies from the reputational harms associated with privacy and data security incidents. In short, indemnification clauses are a good idea, but they are no substitute for ensuring that you are hiring a vendor with a good compliance program and overseeing your vendor's activities.

- **Consider your vendor's insurance.** Whether or not your vendor has insurance that covers its activities and customers is a critical question for you to determine in the due diligence phase, and potentially an issue that should be reflected in your contract. You should consider coverage not only for the vendor's own activities, but also for any liability that might flow to companies to whom they provide services.
- **Monitor, monitor, monitor.** Your management of the vendor should not end with the contract, but the contract instead should be viewed as the starting point for active management. Have tools and systems in place to monitor your vendors—for example, conduct regular audits. Keep abreast of developments in the law, trends in litigation, and advancements in technologies so that you can be an informed manager of the vendor.

Conclusion

For communications companies in today's data-driven environment, privacy and data security concerns should be top of mind. For many companies, it may make sense to rely on third parties to manage a variety of activities, ranging from outsourcing individual email or calling campaigns to day-to-day security tasks. However, with the increasingly complex obligations related to privacy and data security, and the similarly complex issues related to third-party liability, companies cannot confuse reliance on third parties to handle these tasks with passing off their own independent legal and regulatory obligations. Robust due diligence up front, careful contracting, and close and consistent oversight are necessary to help ensure that third-party vendors help to mitigate risk instead of creating unwanted liability. ■

Endnotes

1. Fed. Trade Comm'n, Privacy & Data Security Update: 2016 1 (2016), *available at* https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2016/privacy_and_data_security_update_2016_web.pdf [hereinafter FTC Privacy and Security Update]; 15 U.S.C. § 45(a)(1) ("Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.").
2. FTC Privacy & Data Security Update, *supra* note 1, at 1.
3. 15 U.S.C. §§ 44, 45(a)(2).
4. One interpretation of the exception is that it is based on an entity's status as a common carrier and therefore extends to *all* activities of a common carrier. *See, e.g.*, Fed. Trade Comm'n v. AT&T Mobility LLC, 835 F.3d 993, 1003 (9th Cir. 2016), *reh'g en banc granted*, 864 F.3d 995 (9th Cir. May 9, 2017) **|**; Fed. Trade Comm'n v. Miller, 549 F.2d 452, 456–57 (7th Cir. 1977). A competing interpretation of the exception is that the FTC's jurisdiction reaches common carriers if those entities are not engaged in common carriage activities. *See, e.g.*, Fed. Trade Comm'n v. Verity Int'l, Ltd., 443 F.3d 48 (2d Cir. 2006).
5. *See* Restoring Internet Freedom, Declaratory Ruling, Report & Order, and Order, WC Docket No. 17-108, FCC 17-166 (rel. Jan. 4, 2018) (removing broadband Internet access from common carrier regulation); U.S. Telecom Ass'n v. FCC, 825 F.3d 674 (D.C. Cir. 2016) (approving previous classification of broadband Internet access service as a common carrier service), *reh'g en banc denied*, 855 F.3d 381 (D.C. Cir. 2017) (*USTelecom*). Multiple petitions for certiorari of the *USTelecom* decision have been filed and, as of this writing, remain pending. In addition, numerous parties have pledged to file judicial challenges to the FCC's 2018 order reclassifying broadband Internet access service as a non-common carrier service.
6. 47 U.S.C. § 551.
7. *Id.* § 338(i).
8. *See id.* § 551(a)–(b); *id.* § 338(i)(1), (3)(a).
9. *See id*. § 338(i)(5).
10. *See id.* § 338(i)(6).
11. *See id.* § 222.
12. *See* 47 C.F.R. § 64.2003.
13. *See id.* § 64.2004.
14. *See* TerraCom, Inc. & YourTel Am., Inc., Notice of Apparent Liability for Forfeiture, 29 FCC Rcd. 13325 (Oct. 24, 2014).
15. *See Complying with COPPA: Frequently Asked Questions*, Fed. Trade Comm'n, § A.1 (Mar. 2015), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General Questions [hereinafter *FTC COPPA Compliance Guide*].
16. *See id*.
17. *See* Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Changes: Recommendations for Businesses and Policymakers 58 (Mar. 2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.
18. *See* 47 U.S.C. § 227.
19. *See* 47 C.F.R. § 64.1200(a)(1)–(3).
20. *See* 16 C.F.R. § 310.1 et seq.; *Complying with the Telemarketing Sales Rule*, Fed. Trade Comm'n, Intro. (June 2016), https://www.ftc.gov/tips-advice/business-center/guidance/complying-telemarketing-sales-rule#Introduction.
21. *See* 47 C.F.R. §§ 64.1200, 64.1601(e).
22. *See* 15 U.S.C. § 7701 et seq.
23. *See, e.g.*, Ind. Code § 24-4.9-3-3.5; Utah Code § 13-44-201.
24. Cal. Civ. Code § 1798.81.5(b).
25. 201 Mass. Code Regs. 17:03; *see* Mass. Gen. Laws ch. 93H, § 2 et seq.
26. *See* CalOPPA, Cal. Bus. & Prof. Code § 22575 et seq.; DOPPA, Del. Code Ann. tit. 6, § 1201C et seq.
27. *FTC COPPA Compliance Guide*, *supra* note 15.
28. 47 C.F.R. § 64.1200(f)(9), (11).
29. *See, e.g., id.* § 64.1200(a)(7)(iii).
30. DISH Network, Declaratory Ruling, 28 FCC Rcd. 6574, ¶ 1 (May 9, 2013).
31. *Id.* at ¶ 37; *see also* ACA, Declaratory Ruling, 23 FCC Rcd. 559, ¶ 10 (Dec. 28, 2007) ("Calls placed by a third party collector on behalf of that creditor are treated as if the creditor itself placed the call.").
32. 52 F. Supp. 3d 700, 703 (M.D. Pa. 2014); *See also* Gomez v. Campbell-Ewald Co., No. 13-55486, 2014 WL 4654478 (9th Cir. Sept. 19, 2014) (explaining that all

entities in the marketing chain that meet the standards of common law agency can be vicariously liable under the TCPA).

33. 15 U.S.C. §§ 44, 45(a)(2).

34. Telemarketing Sales Rule, 68 Fed. Reg. 4580-01 (Jan. 29, 2003).

35. *CAN-SPAM Act: A Compliance Guide for Business*, Fed. Trade Comm'n (Sept. 2009), https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business.

36. Cal. Civ. Code § 1798.81.5(c).

37. SOHA Sys., Third Party Access Is a Major Source of Data Breaches, Yet Not an IT Priority (2016), *available at* https://web.archive.org/web/20170708053021/http://go.soha.io/hubfs/Survey_Reports/Soha_Systems_Third_Party_Advisory_Group_2016_IT_Survey_Report.pdf?t=1467123126371; *see also Third Party Vendor Breaches Still a Major Cybersecurity Issue in 2016*, SecurityScorecard (July 20, 2016), https://securityscorecard.com/blog/third-party-vendor-breaches-2016-1.

38. *OCR Investigation into Bizmatics Data Breach Is Closed*, HIPAA J. (Aug. 29, 2016), https://www.hipaajournal.com/ocr-investigation-bizmatics-data-breach-closed-3571/.

39. T.A.N. v. PNI Digital Media Inc., Order Granting Motion for Settlement, No. 2:16-cv-00132-LGW-RSB (S.D. Ga. Dec. 1, 2017); *see Staples Unit Strikes Data Breach Deal with CVS Customers*, Law360 (May 25, 2017), https://www.law360.com/articles/928565?scroll=1.

40. Krakauer v. DISH Network L.L.C., No. 1:14-CV-333, 2017 WL 2242952 (M.D.N.C. May 22, 2017), *motion for judgment as a matter of law & remittitur denied*, 2017 WL 4417957 (Oct. 3, 2017); *see DISH Network Hit with $61M Treble Damages after TCPA Trial*, Law360 (May 22, 2017), https://www.law360.com/articles/927109/dish-network-hit-with-61m-treble-damages-after-tcpa-trial.

41. United States v. DISH Network LLC, 256 F. Supp. 3d 810 (C.D. Ill. 2017), *appeal pending*, No. 17-3111 (7th Cir. filed Oct. 6, 2017); *see* Joseph C. Wylie II, Molly K. McGinley & Nicole C. Mueller, *DISH Network Ordered to Pay $280 Million Fine, Damages in Federal TCPA Lawsuit*, Nat'l L. Rev. (June 9, 2017), https://www.natlawreview.com/article/dish-network-ordered-to-pay-280-million-fine-damages-federal-tcpa-lawsuit.

COURTSIDE

Questions of Compelled Speech at the Supreme Court

BY JESSICA RING AMUNSON AND TASSITY S. JOHNSON

Does an individual have a First Amendment right that trumps a state's anti-discrimination laws? What should happen when an individual's First Amendment right *not* to speak conflicts with a state's obligations, under the Constitution, federal law, and its own laws, to protect its citizens from deception in its marketplaces? Two cases currently pending before the Supreme Court present these questions and could have profound implications for the compelled speech doctrine and the government's regulatory authority over the conduct of businesses and service providers.

The first of these cases, *Masterpiece Cakeshop, Ltd. et al. v. Colorado Civil Rights Commission et al.*, involves a confrontation between the Constitution's protections of free speech and free exercise and its promise of equal protection of the laws, as expressed through the longstanding federal and state prohibition of discrimination in places of public accommodation. This widely publicized case asks the Court to decide whether the First Amendment affords Jack Phillips, a bakery owner, the right to refuse to create a cake for Charlie Craig and David Mullins, a same-sex couple, because Phillips' religious beliefs deem the institution of same-sex marriage sacrilegious. Depending on how narrowly drawn the Court's ultimate decision in this case is, the Court may further enshrine, or dramatically upend, the antidiscrimination principle embedded in federal and state public accommodations laws.

This case began when Craig and Mullins went to Masterpiece Cakeshop, Phillips' bakery, in search of a cake for their wedding reception and were informed that Phillips would not sell same-sex couples baked goods for weddings because of his religious beliefs. The Colorado Civil Rights Commission (Commission) determined that Phillips' refusal to sell a wedding cake was sexual orientation discrimination in violation of the State's Anti-Discrimination Act (CADA) and that the First Amendment did not authorize such discrimination in sales to the general public. The Commission ordered Phillips to stop refusing to sell same-sex couples wedding cakes or any other goods he would sell to heterosexual couples and that order was upheld on appeal.

Jessica Ring Amunson is the co-chair of the appellate and Supreme Court practice at Jenner & Block LLP and Tassity S. Johnson is an associate in the practice group. Ms. Amunson and Ms. Johnson filed an amicus brief in support of respondents in Masterpiece Cakeshop, Ltd. et al. v. Colorado Civil Rights Commission et al.

Phillips challenged this order in the Supreme Court. He asserts that his wedding cakes are extensions of his artistic expression and that one of the core tenets of his religious faith is his belief that marriage is a union between one man and one woman. As a consequence, he argues that his wedding cakes convey messages about marriage that are entitled to the full constitutional protection of the First Amendment. The Commission's order, Phillips charges, forces him to choose between creating cakes that celebrate an institution that offends his religious convictions and forgoing his wedding business in its entirety, and thus violates the Court's prohibition of government action that compels an individual to express the viewpoint of the state.

The couple and Colorado have each filed briefs defending the Commission's order. Both parties argue that the core issue presented by this case is not whether wedding cakes are protected expressive conduct, but rather whether businesses open to the general public can discriminate in their commercial conduct against individuals protected by a state's antidiscrimination laws if they sell an artistic product. Colorado, they contend, seeks to regulate Phillips' commercial conduct, not his viewpoint or expression, and the Court, they note, has consistently upheld antidiscrimination laws in the face of similar constitutional challenges by commercial entities providing expressive goods or services.

Nearly half of this country's states and the District of Columbia expressly prohibit sexual orientation discrimination in places of public accommodation; even more states and the federal government prohibit racial, religious, and gender-based discrimination. A ruling from the Court that creates a religious exemption to these certain aspects of these laws may prove consequential for their continued efficacy.

National Institute of Family and Life Advocates et al. v. Xavier Becerra, Attorney General, et al.—the second of the Court's compelled speech cases this term—could similarly be a game-changer for laws regulating professional conduct and mandatory disclosures. The case concerns the California Reproductive Freedom, Accountability, Comprehensive Care, and Transparency Act (Reproductive FACT Act), which requires facilities providing family planning or pregnancy-related services to disclose the existence of state programs subsidizing prenatal care, contraception, and abortion and, if true, the facilities' lack of medical licensing. "Pregnancy Centers," or religious organizations that operate for the purpose of persuading pregnant women to give birth, are covered by the Reproductive FACT Act. They have asked the Court to weigh in on whether the disclosure requirements effectively conscript them into directing their clients to contraception and abortion, and thus force them to speak in a way that offends their religious beliefs.

The Centers argue that, because the Reproductive FACT Act explicitly does not apply to facilities that do not have the primary purpose of providing family-planning or pregnancy-related services or to facilities that provide birth control and abortion, the Act effectively applies only to facilities like them, which object to contraception and abortion on religious grounds. They contend that, as a result, the Act targets only them for regulation because of their religious viewpoint and compels only them to advocate the State's views. And they assert that California's interest in providing women with information regarding healthcare that is not misleading addresses a problem that the State has not shown actually exists, and thus is not sufficiently compelling to excuse the Reproductive FACT Act's viewpoint discrimination.

California has defended the Reproductive FACT Act before the Court by arguing that the law does not require any facility to provide information on abortions, or refer any client for abortion or contraception, but instead merely imposes a neutral disclosure requirement. The Court's compelled speech precedent, the State contends, does not bar it from requiring that these facilities make nonideological statements of fact designed to eliminate pregnant women's confusion about the facilities' legal or professional status, or the limited, non-contraceptive and non-abortive services they offer.

At the center of this case is a dispute about how forcefully the First Amendment applies to speech made in a professional context, whether purely factual information has an expressive component and viewpoint, and whether a state's requirement that a service provider professionally disclose factual information also requires the service provider to adopt or endorse the state's expression and viewpoint as its own, in violation of the compelled speech doctrine.

Court watchers will be following both of these cases closely to see how the Court navigates competing constitutional concerns in the context of the compelled speech doctrine. ■

Media Law Diversity Moot Court Competition: Winners and Best Brief

BY SMRITI KRISHNAN AND DWAYNE TREECE

The Forum on Communications Law First Amendment and Media Law Diversity Moot Court Competition, now in its eleventh year, is designed to introduce minority law students to the practice of media law and to many of the lawyers who are active in the media law bar.

The Competition provides participants the opportunity to develop their practical lawyering skills by, among other things, requiring each team of participants to prepare appellate briefs and present oral arguments before prominent judges and media law attorneys regarding timely issues of national significance in the field of media law.

The hypothetical legal issue posed to the 2017–2018 Moot Court Competition participants focused on whether an online media platform that encouraged the uploading and sharing of user-created content through a downloadable application violated the Video Privacy Protection Act—specifically, whether the Act was violated by providing user information, including that of both account holders and general users of the application, to an external data analytics and advertising company that used the information to maximize the media platform's profits by directly marketing products and videos to viewers.

A committee of Forum attorneys scored the participants' appellate briefs. The four teams with the highest scores advanced to the semifinal round of oral arguments during the Forum's Annual Conference. The team with the highest-scoring brief was presented with the "Best Brief" award, and each member of the Best Brief team received $1,000. In addition, all semifinalists received complimentary registration to attend the Forum's Annual Conference, round-trip transportation, and four nights' hotel stay during the Annual Conference.

The competition at the Annual Conference resulted in the winning team of Meenakshi Krishnan and Habib Olapeide, both students from Yale Law School, with Meenakshi taking home the coveted title of Best Oralist.

Smriti Krishnan, a student at The University of Alabama School of Law, and Dwayne Treece, a student at Tulane University Law School, were the winners of the 2017–2018 Best Brief award. A copy of Smriti and Dwayne's winning brief is presented here:

IN THE COURT OF APPEALS
FOR THE TWELFTH CIRCUIT
NO. 17-836193

PAUL KATZ,
Appellant,
v.
PENUMBRA MEDIA CO.,
Appellee

ON APPEAL FROM THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF PACIFICA

BRIEF OF APPELLANT

PAUL KATZ

Smriti Krishnan, University of Alabama School of Law

Dwayne Treece, Tulane University Law School

STATEMENT OF FACTS

I. Facts

This case is about how a media giant unlawfully disclosed a subscriber's personally identifiable information ("PII"), including his video-watching history. Paul Katz ("Katz"), a Pacifica resident, is the founder of the Pacifica-based Pacifica Constituents Admiring Transparency and the Press ("PCATS"), an organization that promotes transparency in government and the freedom of the press.[1] Penumbra ("Penumbra") is a video-sharing company and is the creator of the Penumbra app, which delivers its content through a downloadable app that is available to users of Apple and Android devices.

The Penumbra app is free and does not provide for in-app purchases. The process of downloading, installing, and using the app provides viewing access of all channels to any user without the creation of an account. An account is only required for those seeking to upload content, but anyone can create an account for free. Likewise, the app is also free and may be deleted at any time. In its Privacy Policy, Penumbra states the specific information that it gathers:

> **What Information Do We Gather?**
>
> When you use our Penumbra application ("App"), we may gather the information necessary to identify your needs and to provide you with better service. Through your use of the App, we will collect the following information: your GPS location, your unique device ID, and a record of content viewed.
>
> When you register as a user of the App, we will collect the following information: name, email address, cell phone number, demographic information including postal code, Internet Protocol ("IP") Address and other persistent identifiers.

The information collected is to be used *only* for the purpose stated at the time of collection for the purposes stated therein, with Penumbra further noting that it will provide notice to all users if it discloses user data for any other purpose than explicitly stated in its Policy. Penumbra never divulges its intent to disseminate data to third parties for the purpose of advertising or to make a profit.

On the contrary, Penumbra provided its derived subscriber information to an external data analytics and advertising company to monetize this information. Bigoogooloo reviews all user information, including both account holders' and general users' information, to provide Penumbra's content creator channels with direct access to potential viewers. Users were unaware and not given notice of Penumbra's profit-making, unlawful disclosures. Through these connections, Penumbra content creator channels pay Penumbra to directly market products and videos to viewers, maximizing each channel's profits.

Katz is a user of the Penumbra platform because he follows and "likes" content creator channels that promote openness and transparency in government and freedom of the press. Unfortunately, while Katz has never followed or "liked" the Dossier Dawgs channel, which promotes anti-transparency and anti-press messages, Katz receives Dossier Dawgs clips every time the Penumbra app is opened. Katz then learned that Penumbra had unlawfully collected his viewer data and sold it to Dossier Dawgs and other content creator channels. Emotionally disturbed and personally violated, Katz began researching how his data had been unlawfully used by Penumbra and how Penumbra had failed to protect his data. Upon further research, Katz discovered that the data collected by media companies like Penumbra has great value. Katz also discovered that Penumbra had the lowest security out of the top five media companies, increasing the risk of Katz's account being hacked.

II. Procedural History

Katz filed suit against Penumbra following Penumbra's unlawful disclosure of Katz's video-watching history to content creator channels, including Dossier Dawgs. Dossier Dawgs used Katz's private video-watching history to market unwanted health products and push its channel's political agenda on Katz. Penumbra's disclosure of Katz's video-watching history to Dossier Dawgs is a violation of the Video Privacy Protection Act ("VPPA") because the VPPA concretely protects users' video-watching history. Katz argued that he had experienced a personal injury-in-fact as a direct result of Penumbra's VPPA violation. Katz also argued that he had experienced an increased risk of hacking caused by Penumbra's violation. Finally, Katz argued that he had experienced a disclosure of his PII as a subscriber of Penumbra. In response, Penumbra filed a Motion to Dismiss contending that Katz's injuries were not concrete enough to confer Article III standing. Penumbra's Motion to Dismiss also argued that Katz could not sustain his VPPA claim because he did not have any PII disclosed because he was not a "subscriber" of Penumbra. The Pacifica District Court granted Penumbra's Motion to Dismiss under Rule 12(b)(6) because Katz's increased risk of being hacked was found insufficient to sustain an injury-in-fact and because Katz was found not to be a subscriber under the VPPA. The Twelfth Circuit should reverse the District Court of Pacifica's Order Granting Penumbra's Motion to Dismiss under Rule 12(b)(6): Katz has been a victim of Penumbra's disclosure of his video-watching history, making the risk of his account being hacked imminent. Katz also has had his PII disclosed, as a subscriber of the Penumbra app.

SUMMARY OF THE ARGUMENT

Privacy interests are valuable interests already recognized by Congress in a variety of contexts. The legislative intent of the VPPA was to protect video-watching history; any statutory violation of the VPPA through disclosing an individual's video-watching history is therefore a concrete harm. A plaintiff does not have to demonstrate any further facts beyond the unlawful disclosure of his video-watching history: The disclosure itself is the basis to seek redressable relief. The risk of hacking, especially when tied to a present injury-in-fact like the unlawful disclosure of video-watching history, is highly imminent. Courts have not found standing for plaintiffs in the context of future, probabilistic injuries where the harms alleged are entirely speculative.

Katz's Android identification ("ID") number is "personally identifiable information" under the VPPA. Katz and Penumbra have a sufficient relationship for Katz to be a "subscriber" and thus a "consumer" protected by the VPPA. Katz is a subscriber because he arranged for access to Penumbra's video content by downloading, installing, and using the Penumbra app on his smartphone. Katz, like others, viewed video content through free applications such as Penumbra's app on their smartphones and tablets. The safeguards of VPPA did not disappear along with brick-and-mortar video stores. The key assumption of Penumbra's argument—that Katz's app use is equivalent to casually browsing the Penumbra website without logging in—is mistaken. Downloading, installing, and using an app on a smartphone or tablet *is* in fact registering and logging in. A balanced analysis makes it clear that Katz has a persistent subscriber relationship that makes a broad collection of personal information available to Penumbra, triggering the VPPA protection. The VPPA is relevant to modern video consumption, and Penumbra's disclosure of Katz's Android ID number, GPS location, and viewing history is both unlawful and impermissible.

ARGUMENT

I. THE DISTRICT COURT NARROWLY INTERPRETED "INJURY-IN-FACT" TO EXCLUDE KATZ'S IMMINENT RISK OF HACKING TIED TO PENUMBRA'S DISCLOSURE OF VIDEO-WATCHING HISTORY IN VIOLATION OF THE VPPA.

Article III imposes certain limits on judicial power to ensure that the judiciary does not become overly entangled in political disputes.[2] The concern of overly political judiciary entanglement fades when a plaintiff seeks to enforce a personal right

against another party.[3] For a plaintiff to have Article III standing, he must have suffered an injury-in-fact that is "concrete, particularized, and actual or imminent"; the harm suffered must be fairly traceable to the challenged action; and it must be redressable by a favorable ruling.[4] However, the precise boundaries of the standing requirement under Article III are not discernible by any precise test.[5] As changes to the technological landscape create new means of communication, new means of injury that are concrete, though intangible, injuries must be redressable by the Court.[6]

STANDARD OF REVIEW

This Court should apply the *de novo* standard of review to examine the district court's dismissal of the complaint under Rule 12(b)(6) for lack of standing.[7]

A. THE DISTRICT COURT CORRECTLY HELD THAT THE DISSEMINATION OF INCORRECT DATA UNDER THE VPPA IS SUFFICIENTLY CONCRETE TO MEET THE INJURY-IN-FACT ELEMENT OF ARTICLE III STANDING.

Privacy interests have been protected by Congress and the judiciary in several statutory contexts, especially where such interests are implicated by the disclosure of information.[8] The VPPA created a powerful and concrete right to privacy of one's video-watching history.[9] The VPPA authorizes information disclosure only in a limited set of circumstances: ordinary request processing for debt collection activities, order fulfillment, request processing, and transfer of ownership.[10]

Specifically, the disclosure of PII is what Congress explicitly sought to reduce by passing the VPPA into law.[11] Disclosing PII, such as video-watching history, under the VPPA is an injury sufficiently concrete to confer Article III standing.[12] To meet the injury-in-fact element of standing, the plaintiff must seek redress for the wrongful disclosure of information related to him.[13] The VPPA has created a specific right to relief for information disclosures made in violation of the act.[14] The VPPA also notes that wrongful disclosures of information alone are an injury deserving of judicial relief.[15]

In *Austin-Spearman v. AMC Network Entertainment LLC*, the plaintiff user alleged that the television network disclosed personal information in violation of the VPPA.[16] Through the network's website, users accessed website content either as a guest or by using an existing online account.[17] The users' histories were tracked with cookies and then disclosed to other third parties.[18] The network's Motion to Dismiss pursuant to Rule 12(b)(6) was denied because of Congress's ability to confer standing on plaintiffs who experienced a statutory violation of the VPPA.[19]

Katz's situation is highly similar to the plaintiff's in *Austin-Spearman*. Katz discovered that his information—the record of his viewed content along with his GPS location and unique device identification—had been disclosed to content creator channel Dossier Dawgs. Penumbra's disclosure of Katz's video-watching history to Dossier Dawgs for a profit, along with other PII, violates the very legislative purpose of the VPPA and is sufficient to meet the injury-in-fact element of standing.[20] Thus, Katz has experienced a concrete harm.

Katz actually does not have to assert any additional harm beyond Penumbra's disclosure of his video-watching history to Bigoogooloo without his consent.[21] However, this Court should also note that Penumbra has disclosed Katz's PII to a third-party content creator channel beyond the scope of Katz's consent. Penumbra's Privacy Policy explicitly notes that "The information we collect is used only for the purpose we state at the time of collection or for purposes contained below."[22] The disclosure of video-watching history to profit content creator channels was not listed as one of the purposes in the Privacy Policy. Penumbra also did not notify Katz that it was directly giving Dossier Dawgs the chance to market products and videos onto Katz's use of the Penumbra app.[23] Even if this Court does not consider Penumbra's lack of notice to Katz before disclosing congressionally protected video-watching information and the violation of Penumbra's own Privacy Policy, Penumbra's mere disclosure of Katz's video-watching history is sufficient to meet the injury-in-fact requirement under the VPPA.

This Court's affirmation of the district court's judgment that Penumbra's disclosure of Katz's video-watching history aligns with Congress's legislative intent for the VPPA. By recognizing Katz's injury-in-fact, Penumbra's wrongful disclosure of his video-watching history in violation of the VPPA, the Twelfth Circuit would provide Katz redressable relief.

B. THE DISTRICT COURT ERRED IN HOLDING THAT RISK OF HACKING IS SPECULATIVE AS TO DENY ARTICLE III STANDING.

To meet the injury-in-fact requirement of Article III standing, the plaintiff must show the invasion of a legally protected interest that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical."[24] The use of probabilistic injuries to support standing is permitted.[25] Federal courts frequently allow actions for injunctive and declaratory relief, aimed at preventing future activities that are reasonably likely or highly certain, neither standard being absolutely certain.[26] Certainty should not be a touchstone of standing.[27] The Supreme Court has not foreclosed the use of *any* future injuries to support Article III standing.[28] The Supreme Court suggests that the floor for concrete harm is above mere allegations of possible future injury.[29] Therefore, the probability of the future injury may be tied with a present injury.[30]

i. The increased risk of hacking is concrete and particularized.

A "concrete" injury is not necessarily synonymous with a tangible injury.[31] The risk of real harm or intangible injuries can satisfy the concrete harm requirement.[32] Furthermore, the standard for concrete harm does not apply as rigorously when a private plaintiff seeks to vindicate his own private rights.[33] A court may infer that plaintiffs have shown a substantial risk of harm from a prior data breach.[34] To have a "particularized" harm, the plaintiff must demonstrate that he has a personal stake in

the dispute and that he has suffered a harm in a personal and individual way.[35]

Penumbra has already violated the VPPA by providing Katz's video-watching history to Dossier Dawgs for a profit. Only then was Dossier Dawgs able to market products and videos to Katz directly, without his permission. Notably, Katz was only aware that his information had been disclosed in violation of the VPPA after he saw Dossier Dawgs clips appearing on his app. Katz experienced vulnerability after he realized that his account had a greater risk of being hacked with Penumbra's disclosure of his video-watching history. Penumbra's unlawful sale and disclosure of Katz's video-watching history is the present injury Katz experiences, making the future probability of his account being hacked greater. The risk of being hacked is concrete as Katz has already experienced Penumbra's unlawful disclosure of his video-watching history.

Katz has also demonstrated that he has a personal stake in the dispute: He has brought a lawsuit on behalf of himself after experiencing "significant anger, frustration and distress." Katz is concerned with how Penumbra's undisclosed sale of his video-watching history to profit content creator channels will affect the security of his usage of the Penumbra app. Katz's research into the probability of his data being hacked emphasizes the personal stake he has in the dispute, strengthening the argument that his harm meets the particularized standard.

ii. The increased, future risk of hacking is actual or imminent. Appellate courts have generally recognized that an increased risk of future injury can satisfy Article III where the increased risk of injury is credible and not conjectural.[36] Various decisions encompass a variety of factors that the Circuits have considered prior to deciding whether a harm is imminent.[37]

The nature of Katz's future risk is the imminent breach of his PII, including his video-watching history, which Penumbra collects and discloses to Bigoogooloo, Inc. There is nothing in the facts to suggest that Penumbra attempted to stop the disclosure of Katz's video-watching history. The plausibility of the future risk of hacking Katz's account is tied to Penumbra's unauthorized disclosure under its own privacy policy and the VPPA itself: By disclosing Katz's video-watching history to Dossier Dawgs, Penumbra has increased the risk of Katz's account being hacked. PCATS is an organization diametrically opposite in its purpose to Dossier Dawgs. Gaining access to Katz's viewer-watching history and his personal information would be a gold mine for a hacker: As the founder of PCATS, Katz is an especially vulnerable plaintiff because he is well-known in the media industry and at the vanguard of digital technology.

Furthermore, Katz's reliance on research to demonstrate how concrete the imminent risk of his account being hacked is aligns well with media industry standards. Research to keep technology providers aware of industry-wide practices in maintaining security is not a radical concept.[38] Katz acknowledges the risk of his account being hacked has increased by citing studies and controlled experiments.

Courts have only denied standing where the injury under consideration is not imminent and where plaintiffs attempt to prove that they have met the imminent aspect of a harm through pure extrapolation or speculation.[39] The Ninth Circuit found a credible threat of harm where employees of Starbucks had their laptop with social security numbers, names, and addresses stolen.[40] The threat of a hacker potentially accessing all of the plaintiffs' PII was considered sufficient to be an injury-in-fact.[41] The plaintiffs' injury-in-fact was their increased risk of future identity theft.[42] The Ninth Circuit did not require absolute certainty to recognize the increased risk that the plaintiffs faced.

On the other end of the extrapolation spectrum, the plaintiff business owners in *Storino* alleged purely speculative harms.[43] The plaintiff business owners claimed that they could become injured because their current rooming and boarding house and hotel use would eventually be zoned out of existence.[44] The plaintiffs argued that they would have to seek a variance for any modifications to their property in the future.[45] The business owners did not assert that their property fell under the scope of the ordinance or that they would eventually be affected by the ordinance.[46] The Third Circuit noted that the plaintiffs had no allegation that was imminent, only pure speculation.[47]

Katz's increased risk of imminent harm is closer to the *Krottner* plaintiffs, and further away from the *Storino* plaintiffs.[48] Much like the *Krottner* plaintiffs, Katz's injury-in-fact is the increased risk or threat of hacking that he faces stemming from Penumbra's low-level security and prior disclosures of his video-watching history. Unlike the *Storino* plaintiffs who lacked standing, Katz does not have to rely on pure speculation to allege an imminent harm: He has already experienced a concrete VPPA violation by Penumbra. Penumbra's VPPA violation gave Dossier Dawgs, a party that Katz does not know, direct access to Katz's video-watching history and other PII collected.

Even if this Court were to adopt a narrower view on the injury-in-fact requirement, the imminent increased risk of hacking Katz experiences meets Article III standing requirements because the increased risk of hacking is not entirely speculative or extrapolative. Primarily, Penumbra's disclosure of Katz's video-watching history has threatened Katz with a loss of information, including PII collected from Katz.[49] Penumbra's actual, unlawful disclosure and sale of Katz's video-watching history to profit Dossier Dawgs is substantially more than mere allegations of an increased risk of future hacking.[50]

As a policy matter, there is generally no danger that a private party suit is an impermissible attempt to police political activity.[51] The lesser likelihood of a private party seeking relief for a political gain may be a reason why district courts in the Seventh Circuit have determined the claims of increased risk of identity theft due to hacking confer standing on the plaintiffs attempting to meet the injury-in-fact element.[52] After being personally violated by Penumbra's

disclosure of his video-watching history and taking the trouble to substantiate his violation with research, Katz filed the lawsuit in a personal capacity, and not in his capacity as the founder of PCATS. Recognizing that Katz's risk of being hacked as a concrete, particularized, and imminent injury would not broaden the existing requirements of standing. In Katz's case, his increased risk of being hacking is tied to the unlawful disclosure of his video-watching history under the VPPA.[53] The disclosure of Katz's video-watching history is a well-established intangible, concrete harm under the VPPA and its legal progeny. By recognizing that Katz's increased risk of hacking stems from Penumbra's statutory violation of the VPPA, the congressional intent to protect video-watching history would be fulfilled.

The Twelfth Circuit should reverse the district court's finding that Katz lacks standing: The increased risk of hacking that Katz is experiencing is tied to Penumbra's prior unlawful disclosure and sale of Katz's video-watching history to content creator channels.

II. WHILE THE DISTRICT COURT COERRECTLY HELD AN ANDROID ID, GPS DATA, AND VIEWING INFORMATION AS PERSONANNLY IDENTIFIABLE, ITS DISQUALIFICATION OF KATZ'S STANDING AS A "CONSUMER" WAS IN ERROR.

There are two schools of thought with regard to whether disclosed information is PII. The first requires that the information, *by itself*, be directly capable of identifying an individual. Under this approach, a device identifier and GPS as found in this case are not sufficient to constitute PII. The second allows the disclosed data to be combined with and cross-referenced with information held by a third-party source, including data analytics companies. Under this approach, the device identifier and GPS will constitute PII because third-party information can be used to "reverse engineer" and identify a specific individual. The courts have struggled with adapting the somewhat dated VPPA to modern technology.

STANDARD OF REVIEW

The district court's dismissal under Fed. R. Civ. Pro. 12(b)(6) should be reviewed de novo, examining the factual allegations in the complaint as true and construing them in the light most favorable to Katz.[54]

A. THE DEVICE IDENTIFIER, GPS DATA, AND VIDEO-VIEWING INFORMATION JOINTLY ESTABLISH PERSONALLY IDENTIFIABLE INFORMATION UNDER THE VPPA.

Subject to certain exceptions, the VPPA prohibits "video tape service providers" from knowingly disclosing, to a third-party, "personally identifiable information ('PII') concerning any consumer of such provider."[55] The term PII includes "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider."[56] Ultimately, whether the information that has been disclosed qualifies as PII depends upon the type of information disclosed and how many steps removed that piece of information is from an individual's identity.

Because the data that are provided to Bigoogooloo is readily cross-referenced across Bigoogooloo's database, this situation is more closely aligned with the second school of thought, as illustrated in the court's reasoning in *Yershov*.[57]

In *Yershov*, a user of the *USA Today* app alleged that each time he viewed a video clip, the app transmitted his mobile Android ID, GPS coordinates, and identification of the watched video to a third-party analytics company to create user profiles for the purposes of targeted advertising, all in violation of the VPPA. Despite dismissing the complaint, the lower court had found that while the disclosure of the GPS coordinates, Android ID, and video history were enough to constitute "personally identifiable information" (PII) under the VPPA, a third-party analytics company could still use the data disclosed by the defendant to identify individuals and their viewing habits merely because the plaintiff, as the user of a free app, was not a consumer.[58]

In the case at hand, each time Katz viewed a video clip, the app transmitted his mobile Android ID, his GPS coordinates, and identification of the watched video to a third-party analytics company, Bigoogooloo, to create user profiles for the purposes of targeted advertising, all in violation of the VPPA. If the app disclosed only a device identifier and viewing history, and nothing more, the information is isolated. In many cases, a device identifier on its own cannot lead to an individual.[59] Here, the device identifier alone would have allowed the user to remain anonymous. However, GPS coordinates are included in this disclosure. GPS coordinates make identifying a particular individual much easier. This information is easily cross-referenced with data held at an analytics company like Bigoogooloo. Even ignoring Bigoogooloo's involvement, it is possible with a few clicks of a mouse to generate an address. Additional online searching can unmask the identity of an individual user with relative ease. As a result, the information disclosed should be considered PII under the VPPA.[60]

While Penumbra asserts that the information it disclosed to Bigoogooloo, Inc., was not PII under the VPPA, the district court ably dismantled this and concluded that persistent, unique device identifiers like Android ID, especially when paired with GPS coordinates and video viewing information, are PII protected by the VPPA.

The transaction described in the complaint—whereby Katz used the mobile device application that Penumbra Media Co. provided to him, which gave Defendant the GPS location of Plaintiff's mobile device at the time he viewed a video, his device identifier, and the titles of the videos he viewed in return for access to Defendant's video content—plausibly pleads a case that the VPPA's prohibition on disclosure applies.

B. KATZ IS A "SUBSCRIBER" WHO QUALIFIES AS A CONSUMER UNDER THE VPPA BECAUSE AN EXCHANGE OF VALUABLE INFORMATION CONSTITUTES CONSIDERATION AND A PERSISTENT, DURABLE RELATIONSHIP WITH

PENUMBRA.

Only a "consumer" can bring an action under the VPPA.[61] The VPPA provides that a "consumer" is defined as "any renter, purchaser, or subscriber of goods or services."[62] The VPPA does not contain further definitions for any of these terms and a review of the legislative history sheds no further light on the meaning of "subscriber." To determine whether Penumbra users are customers under the VPPA, Katz's use of the app must be qualified within the meaning of the term "subscriber." Absent this statutory information, it is assumed that the plain and ordinary meaning of the term guides its definition.

i. Although the Penumbra app does not require payment, its users are still subscribers under the VPPA due to the valuable personal information exchanged as consideration.

The *Merriam-Webster's Collegiate Dictionary* defines a "subscriber" as one who subscribes to a thing.[63] The dictionary further notes that "subscribe" means "to enter one's name for a publication or service."[64] In the context of the VPPA, the term "subscribe" encompasses "renter" and "purchaser," which both presume that payment *or* consideration is given in exchange for a service. Because the plain definition of "subscriber" combines these definitions, the district court erred in its opinion that a subscriber requires a paid subscription. In the "modern electronic world, subscriptions entail a broader spectrum of activity."[65]

Correspondingly, *In re Hulu* held that users of an online streaming source who visited a website, registered, and viewed content met the requirements of "subscribers" and were deemed consumers under the VPPA.[66] Relying on the ordinary meaning of the terms "renter," "purchaser," and "subscriber," *Hulu* concluded that payment was not required to meet any arbitrary definition of "subscriber" as Congress could have limited the word "subscriber" by describing it as a "paid subscriber."

While Katz has paid no money nor opened an account, he is a "consumer" under the VPPA because his access to the app was not free of a commitment to provide consideration in the form of information, which was of value to Penumbra. By installing the app on his phone and establishing seamless access to an electronic version of Penumbra Media, Katz established a relationship that is materially different from that had he simply accessed one of millions of sites on the web through a web browser, despite not paying Penumbra or registering his information. Katz meets the definition of subscriber, and thus "consumer" under the VPPA because he provided a trove of valuable user information, thereby establishing consideration. Therefore, this Court should correct the district court's ruling, following the guidance of *In re Hulu*.

ii. Downloading, installing, and using the Penumbra app on his smartphone created the kind of persistent, durable relationship between Katz and Penumbra sufficient to render him a subscriber.

Generally, individuals using free mobile applications to view free content have not been deemed subscribers under the VPPA without additional facts establishing a stronger relationship.[67] A persistent relationship is formed when a consumer "register[s] with a provider or *otherwise provide[s] his name and address or similar personal information*."[68] However, in comparing app usage to casual Internet browsing,[69] Penumbra and the district court overlook critical distinctions between the two. Penumbra asserts that because Katz did not provide it with the sort of information that would be provided through a registration or sign-up process, he is essentially the same as a casual web surfer, who is not a subscriber under the VPPA.[70] Because users can delete the Penumbra app and do not need to create lasting accounts, its users are not subscribers under the VPPA.

By arranging for access to content through the Penumbra app, Katz has established a relationship with Penumbra. Downloading, installing, and running an app on one's mobile device creates exactly the type of relationship that the district court believed was missing.[71]

Suggesting that personal information of the same kind constitutes consideration enough, the First Circuit contends that such a durable, persistent relationship is unnecessary.[72] However, given the district court's misconception of subscriptions and subscribers, and its misinterpretation of such under the law, the analysis will turn on the district court's misuse of *Ellis*. Under *Ellis*, watching clips on a mobile app without creating a commitment or relationship between the user and app provider did not constitute subscribing, particularly where the user could easily delete the app without consequence or never access it in the future.[73] Similar to the *Ellis* app provider, Penumbra wrongfully argues that the transient nature of users disqualifies Katz as a subscriber. Because there is an exchange of device identifiers for service and the advertising profits Penumbra makes after seeking new users, the strong relationship standard *Ellis* articulated for a user to be a "subscriber" is met.

Crucially, the Penumbra app permits Penumbra to learn far more about Katz than it could find out about him had he only visited Penumbra's website. Indeed, the mobile app enables Penumbra to access the same information about Katz that it presumably would obtain through a formal registration process.[74] For example, a typical registration form might collect a user's name: Android users' first and last names are stored on their phones and accessible to apps.[75] With an app, providing personal and contact information through a registration or sign-up process is unnecessary because the app already can communicate with its users and access their personal information through the app. Once Katz downloaded and installed the Penumbra app on his phone, he was de facto registered, and thus a subscriber.[76]

Regarding credit card numbers, the Penumbra app provides an integrated way to collect payment that does not require a Penumbra-specific registration.[77] The Penumbra app can also use the phone's GPS to figure out a consumer's precise location; Katz's precise location is tracked through this method. Katz did not need to register by his email address: Such an address would be superfluous because

an app simply can display notifications directly on the consumers' phones as the Penumbra app does.[78] By downloading and installing the Penumbra app on his smartphone, Katz provided Penumbra with access to precisely the kinds of information a traditional subscriber would provide through a registration or sign-up process. While some apps do require formal registration, it is simply another way to facilitate the same exchange of information. By contrast, Penumbra cannot collect this information about Katz through the Penumbra website because a browser does not provide similar access to personal information.

Contrary to the district court's opinion, the downloading of an app is not the equivalent of adding a particular website to one's Internet browser as a favorite, allowing quicker access to the website's content. Arranging access to content, the very action Katz took, is the modern equivalent of placing a newspaper holder on a mailbox, while reading the website is the modern equivalent of picking up the paper from a hotel lobby. The former creates a subscriber relationship; the latter does not. Katz falls into the former category. Downloading, installing, and using the Penumbra app on his smartphone created the kind of persistent, durable relationship between Katz and Penumbra sufficient to render him a subscriber.

CONCLUSION

This Court should award Katz relief because, as a subscriber of the Penumbra app, Katz has experienced an increased vulnerability tied to the imminent risk of hacking. Penumbra has caused this imminent risk of hacking because of its unlawful disclosure and sale of Katz's device identifier, GPS, and video-watching history to third-party content creator channels without notice to Katz. Penumbra has violated the very legislative intent of the VPPA and its own Privacy Policy. Katz has experienced a sufficient injury-in-fact under Article III's standing requirement to bring his case forward. ■

Endnotes

1. Editors' Note: This brief's Table of Authorities and many excellent citations to the "Record" and the "District Court Opinion below" have been removed for readability.

2. *See* U.S. Const. art. III, § 2, cl. 1; Warth v. Seldin, 422 U.S. 490, 498 (1975).

3. Spokeo, Inc. v. Robins, 136 U.S. 1540, 1551 (2016) (Thomas, J., concurring).

4. *See* Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992); Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 140 (2010).

5. Clapper v. Amnesty Int'l U.S.A., 568 U.S. 398, 423 (2013) (Breyer, J., dissenting).

6. *See Spokeo, Inc.*, 136 U.S. at 1549.

7. Allco Finance Ltd. v. Klee, 861 F.3d 82, 94 (2d Cir. 2017); Finkelman v. NFL, 810 F.3d 187, 194 (3d Cir. 2016); B.C. v. Mount Vernon Sch. Dist., 660 F. App'x 93, 95 (2d Cir. 2016).

8. *See* Electronic Communications Privacy Act, 18 U.S.C. § 2510 (2002) (creating more stringent standards for governmental surveillance of the public); Stored Communications Act, 18 U.S.C. § 2703 (2016) (restricting Internet service providers' disclosure of subscribers' stored, electronic content); United States DOJ v. Reporters Comm. for Freedom of Press, 489 U.S. 749, 751–53 (1989) (where the criminal records were restricted to only government use and Congress's authorized release of such records for very limited purposes).

9. Video Privacy Protection Act, 18 U.S.C. § 2710 (2013). *See also* Yershov v. Gannett Satellite Network, Inc., 820 F.3d 482, 486–87 (1st Cir. 2016) (holding that the VPPA protected a user's identity where personally identifiable information like video titles and unique device identifiers was reasonably and foreseeably likely to establish the user's identity).

10. Sterk v. Redbox Automated Retail, LLC, 770 F.3d 618, 621 (7th Cir. 2014).

11. *See id.* at 623 (noting, "every court to address this question has reached the same conclusion").

12. *Id.*

13. Spokeo, Inc. v. Robins, 136 U.S. 1540, 1555 (2016).

14. Austin-Spearman v. AMC Network Entm't LLC, 98 F. Supp. 3d 662, 668 (S.D.N.Y. 2015).

15. *Id.* at 666. *See also In re* Hulu Privacy Litig., 86 F. Supp. 3d 1090, 1095 (N.D. Cal. 2015).

16. *Austin-Spearman*, 98 F. Supp. at 663.

17. *Id.* at 664.

18. *Id.*

19. *Id.* at 666.

20. *See* 18 U.S.C. § 2710; S. Rep. No. 100-599, 2d Sess., at 5 (1988); *Austin-Spearman*, 98 F. Supp. at 666.

21. Fed. Election Comm'n v. Atkins, 524 U.S. 11, 20–25 (1998).

22. *Id.*

23. *See In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 272–75 (3d Cir. 2016) (noting that the unlawful disclosure of legally protected information is a de facto injury even in the midst of a circuit split on whether the disclosure of PII to a third party without consent satisfies the concrete injury requirement under Article III).

24. Spokeo, Inc. v. Robins, 136 U.S. 1540, 1548 (2016) (citing Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (2010)).

25. Duke Power Co. v. Carolina Envtl. Study Grp., Inc., 438 U.S. 59, 98 (1978).

26. Clapper v. Amnesty Int'l U.S.A., 568 U.S. 398, 431 (2013) (Breyer, J., dissenting).

27. *Id.*

28. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 668, 693 (7th Cir. 2015).

29. *Clapper*, 568 U.S. at 1147.

30. *Id.* at 437 (Breyer, J., dissenting) (pointing out the majority rationale in its analysis of standing).

31. Spokeo, Inc. v. Robins, 136 U.S. 1540, 1549 (2016).

32. *Id.* at 1549; *see also* Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 154–55 (2010) (recognizing the possibility of having genetically modified alfalfa seeds was a sufficiently concrete harm where farmers needed to test their alfalfa seeds to see whether they were genetically modified).

33. *Spokeo*, 136 U.S. at 1552.

34. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 668, 693 (7th Cir. 2015) (reasoning that a court may need to make an inference to recognize a substantial risk of harm the plaintiffs experienced after one data

breach in the security).

35. Raines v. Byrd, 521 U.S. 811, 819 (1997); *see also* Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (2010).

36. Riva v. Pepsico, Inc., 82 F. Supp. 3d 1045, 1052 (2015); *see also* Mountain States Legal Found. v. Glickman, 92 F.3d 1228, 1234–35 (D.C. Cir. 1996) (recognizing that the Forest Service's action caused a steady increase in the risk of forest fires occurring); Central Delta Water Agency v. United States, 306 F.3d 938, 947–48 (9th Cir. 2002) (plaintiffs were allowed to proceed with their lawsuit concerning whether they would suffer a substantial risk of harm as a result of the government's environmental policies).

37. *See Monsanto*, 561 U.S. at 153 (suggesting that one factor in determining the imminent aspect of a harm could be whether the defendant's allegedly wrongful behavior will likely occur or continue).

38. *See In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1206–07 (N.D. Cal. 2014).

39. *See* Clapper v. Amnesty Int'l U.S.A., 568 U.S. 398, 402 (denying standing to plaintiffs because they merely suspected governmental interceptions occurred); *Lujan*, 504 U.S. at 563–65 (denying standing to plaintiffs who were unable to articulate when they would visit wildlife reserves affected by federal regulations).

40. Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010).

41. *Id.* at 1142.

42. *Id.*

43. Storino v. Borough of Point Pleasant Beach, 322 F.3d 293, 295 (3d Cir. 2003).

44. *Id.*

45. *Id.*

46. *Id.* at 296–97.

47. *Id.* at 298. *See* Cahen v. Toyota Motor Corp., 147 F. Supp. 3d 955, 958 (N.D. Cal. 2015) (discussing the necessity of understanding the plausibility of future risk for standing purposes).

48. *See* Reilly v. Ceridian Corp., 664 F. 3d 38, 44 (3d Cir. 2011) (suggesting a sliding scale of alleged harm to determine injury-in-fact after comparing the plaintiffs' injury-in-fact to that of the plaintiffs in *Pisciotta v. Old National Bancorp.* and *Krottner v. Starbucks Corp.*, from the Seventh and Ninth Circuits respectively).

49. *See* Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1048 (E.D. Miss. 2009).

50. *See* Pisciotta v. Old Nat'l Bancorp., 499 F.3d 629, 639 (7th Cir. 2007).

51. Spokeo, Inc. v. Robins, 136 U.S. 1540, 1553 (2016).

52. *Pisciotta*, 499 F.3d at 1051.

53. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 668, 695 (7th Cir. 2015) (denying standing where plaintiffs were not able to demonstrate that the loss of their private information was an intangible injury).

54. Butler v. Balolia, 736 F.3d 609, 612 (1st Cir. 2013).

55. 18 U.S.C. § 2710(b)(1) (2013).

56. *Id*. § 2710(a)(1), (3).

57. Yershov v. Gannett Satellite Network, Inc., 820 F.3d 482, 486 (1st Cir. 2016).

58. *Id.*

59. *See* Robinson v. Disney Online, 152 F. Supp. 3d 176, 179 (S.D.N.Y. 2015) (holding the video-watching information disclosed must connect a particular individual with the disclosed viewing history).

60. *Id.*

61. 18 U.S.C. § 2710(a)(1) (2013).

62. *Id.*

63. *See Subscribe*, Merriam-Webster's Collegiate Dictionary 1244 (11th ed. 2012); Austin-Spearman v. AMC Network Entm't LLC, 98 F. Supp. 3d 662, 669 (S.D.N.Y. 2015) (noting that "subscription" is an exchange where the subscriber and provider derive monetary or nonmonetary benefits from one another).

64. *Subscribe*, *supra* note 63.

65. Yershov v. Gannett Satellite Info. Network, Inc., 104 F. Supp. 3d 135, 144 (D. Mass. 2015), *rev'd*, 820 F.3d 482 (1st Cir. 2016) (providing personal information constituted consideration).

66. *In re* Hulu Privacy Litig., No. C 11-03764 LB, 2012 WL 3282960 (N.D. Cal. Aug. 10, 2012).

67. Ellis v. The Cartoon Network, Inc., 803 F.3d 1251 (11th Cir. 2015).

68. *Id.* at 1256; Austin-Spearman v. AMC Network Entm't LLC, 98 F. Supp. 3d 662, 669 (S.D.N.Y. 2015).

69. *See Ellis*, 803 F.3d at 1257 ("The downloading of an app, we think, is the equivalent of adding a particular website to one's Internet browser as a favorite, allowing quicker access to the website's content.").

70. *Id.* at 1256 (a subscriber relationship is "one generally undertaken in advance and by affirmative action on the part of the subscriber, so as to supply the provider with sufficient personal information to establish the relationship and exchange" (quoting *Austin-Spearman*, 98 F. Supp. 3d at 669)).

71. *Austin-Spearman*, 98 F. Supp. 3d at 669 (finding no "subscriber" relationship because plaintiff did not, for instance, "download an app or program").

72. Yershov v. Gannett Satellite Info. Network, Inc., 104 F. Supp. 3d 135, 144 (D. Mass. 2015).

73. *See Ellis*, 803 F.3d at 1251, 1257.

74. *See* Noah Feldman, *What You Watch on Your Phone Might Not Be Private*, BloombergView (Oct. 12, 2015), http://bv.ms/1GEzPSI (noting that a "login wouldn't have told [the *Ellis* defendant] any more than it could find out" already about its app users).

75. Alex Mullis, *Android App Permissions Explained*, Android Auth. (Sept. 25, 2015), http://goo.gl/o64WEC.

76. *Id*.

77. *In-app Billing Overview*, Android, http://goo.gl/B2Koj.

78 *See Notifications*, Android, http://goo.gl/q1I1U.

Book Review—*The Right of Publicity: Privacy Reimagined for a Public World*

BY STEPHANIE S. ABRUTYN

Jennifer Rothman's *The Right of Publicity: Privacy Reimagined for a Public World* is a fascinating read for anyone who is interested in the nuts and bolts of right of publicity law and how the doctrine evolved to where it is today. It also will serve as a valuable resource for litigators looking for guidance on how to reconcile the seemingly contradictory precedent in a way that is understandable.

The book takes a historical approach to establishing a framework for what right of publicity law should look like by exploring why we need such a right and what its objectives are. Ultimately, Rothman makes a compelling case for going back to the past.

Rothman starts by tracing the origins of the right of publicity to the invention of the first Kodak portable camera. She debunks many myths about the early law by doing a deep dive into the cases that prompted the first legislation, with specifics that are not well known, even if one is familiar with the cases themselves. Particularly interesting given today's ongoing legislative activity, which includes efforts to amend the New York state statute (SAG is advocating to expand the right while the Hollywood studios oppose), is the early role played by lawyers from the studios, including then in-house counsel to Paramount Melville Nimmer, to advocate for a transferable right of publicity. Baseball cards and Al Capone also make appearances, before Zacchini and Elvis.

By going back to the source material instead of relying on commentary, Rothman determined that much of the reporting about the early cases appears to be fatally flawed. In some cases, articles reported the wrong outcome; in others, cases were criticized extensively for something the court never actually said. She takes some not-so-backhanded slaps at the Harvard and Yale law reviews, supporting her position effectively with detailed citations to the underlying material.

After nearly 75 pages of rich historical detail, Rothman dives into Prosser's well-known and influential 1960s article "Privacy," where he first presented the idea that the right of privacy is really four different torts, and where the concept that misappropriation (right of publicity) is a privacy right took hold in modern jurisprudence. This is where the book truly begins to lead us to where right of publicity doctrine sits today. Rothman goes on to summarize the "breadth and variability" of current right of publicity law around the country and traces it back to the historical discussion in the early chapters.

The fundamental thesis of the book is Rothman's view that there is a misunderstanding about the underlying basis for right of publicity law and that divergence from the doctrine's privacy origins has led to the current doctrinal mess. She cites *Zacchini v. Scripps-Howard Broadcasting Company*, 433 U.S. 562 (1977), as the original culprit responsible for today's inconsistency because it was the first decision that overlaid the property-based framework of intellectual property rights on the "appropriation" torts. Even if the reader is not convinced that the current doctrinal confusion can be so neatly explained, Rothman makes a compelling argument for why the privacy framework, rather than the intellectual property framework, is the right one, and could be the best solution for the future.

The book also does an excellent job of outlining why a truly transferable right of publicity would be problematic in many ways. Of particular concern to Rothman is the escalating conflict between right of publicity claims and the First Amendment. Efforts, sometimes successful, to use right of publicity law to control or penalize commentary about real people in expressive works would be reined in by the more speech-protective privacy approach. Reframing right of publicity law to focus on the actual harm rather than the concept that an individual should be compensated for the use (or value) of his name or likeness, Rothman posits, also would solve some of the conflict with copyright law. According to Rothman, the confusion that is today's right of publicity doctrine and the resulting threat to free expression is a result of the tort drifting into the intellectual property bucket, and going back to the past and focusing on the privacy roots of the right of publicity doctrine is the best way to undo that damage.

The Right of Publicity: Privacy Reimagined for a Public World is a compact read that connects the dots among seemingly irreconcilable court decisions and presents a framework for cleaning up the inconsistency in a way that does not impinge on free speech. This book will quickly become one of the most cited sources by litigants and courts grappling with right of publicity issues. ■

The Right of Publicity: Privacy Reimagined for a Public World

Jennifer E. Rothman
Harvard University Press
256 pages; $39.95 (hardcover)

The Differing US and EU Regulatory Responses cont'd

Continued from page 1

though 27 percent of US chief executives are women.[3]

As the *Times* noted, the reason for these results is not clear. Some advertisements may appear because the advertiser is targeting men.[4] It is also possible that the algorithmic agents used to place the ads had determined that men were more likely to click on the ads than women. There is another possibility: The research findings may demonstrate that algorithmic software is not free of human influence, but rather reflects discriminatory impulses, beliefs, and habits of thinking of online users.

There are many reasons why the use of algorithmic agents has increased, but, as scholars have noted, perhaps the largest factor is the increasingly centralized communication infrastructure, which includes Facebook for social networking, Google for searching and advertising, Amazon for online retail and cloud services, and Apple in mobile hardware and software.[5] These providers collect vast troves of personal data that can be used effectively to model algorithmic processing agents and deliver to individuals a personalized online cocoon.

Engineering Out Harmful Effects of Algorithms Is Not Easy

Despite growing awareness of the power and potentially harmful effects of algorithmic processing agents, there is little real understanding of how algorithms work. Research has postulated several reasons for this "control crisis," including a lack of empirical knowledge of our algorithmically personalized digital environment.[6] Put differently, scientists "lack systematic insight into what is happening inside the individual experience cocoons and how those events aggregate on a societal level."[7] We also have not reached consensus on how to even monitor what is happening within the algorithmic decision-making process.[8] From end to end—from algorithm to user experience—the process by which profiling decisions are made and how they are experienced by users is something akin to a black box.

More critically, it is difficult to even test algorithms. Discriminatory algorithmic decisions "are not hard-coded, and may be the emergent properties of the machine learning process, not identifiable from the review of code."[9] In fact, it is difficult for scientists to directly access algorithmic code, which is typically treated as trade secret material by technology companies.[10] Even with a fully transparent code, "the inner workings of an algorithmic agent may remain unintelligible for humans, making the *a priori* scrutiny hard, if not impossible."[11]

Because a ready engineering solution to lessen the potential negative impacts of algorithms may not be at hand in the near future, we turn to legal efforts to regulate the use of algorithms. We will focus on divergent approaches in the United States and EU to address this issue.

The US Limited Approach Toward Regulating the Use of Algorithms

The legal response in the United States to the potential problems of algorithmic profiling has been scant, sectorial, and reliant on a traditional harm-based approach toward regulation. Take for instance one of the most ubiquitous kinds of online algorithmic processes: online behavioral advertising. Notably, the FTC—the primary privacy and data security regulator in the United States—has not come close to suggesting that online behavioral advertising should be banned. Rather, the FTC has issued guidelines promoting the goals of transparency and disclosure in the use of targeted advertising, under the theory that informed users can make rational decisions about their online practices.[12] The closest the FTC has come to a ban is to require that US companies obtain consent to use sensitive customer data (health information, information relating to children, financial information, and geo-location data) for online behavioral advertising.[13] Self-regulatory regimes such as the Digital Advertising Alliance likewise stress the need for transparency and disclosure but do not ban the practice or require that web publishers obtain an affirmative opt-in to allow online behavioral advertising.[14]

Not even the State of California, typically at the vanguard of privacy legislation, has materially restricted the use of online behavioral ads. The California Online Privacy Protection Act (CalOPPA) requires companies that do business in California to post online privacy policies that explain the kinds of personal information they collect and share with third parties—in addition to the personal information collected by third parties.[15] CalOPPA also requires that companies disclose in their privacy policy how they respond to browser "do not track" signals.[16] The law, however, does not require California businesses to honor do not track requests or provide for opt-outs from tracking. No law in the United States imposes a blanket requirement that online users affirmatively opt in to browser cookies or online behavioral advertising.

Federal regulators have recognized the potential for discriminatory impact arising from the use of algorithmic agents, under fair credit laws such as the Fair Credit Reporting Act or the Equal Credit Opportunity Act.[17] Regulators, for example, have cautioned that the use of social media connections/relationships, academic records/educational background, job type/status, online shopping purchase patterns/behaviors, website subscriptions, GPS/location data, and IP address can lead to discriminatory profiling and may be problematic in the context of automated lending or housing decisions.[18] But to date there has been no US law that specifically bans the use of data or algorithms to make decisions about credit or housing or employment, only a prohibition on using the data in a discriminatory way that would violate existing laws.

EU Heightened Approach

The approach in the EU toward

regulating algorithmic agents is far different than in the United States. In contrast to the US, the EU begins with the principle that the processing of any personal data is *presumptively invalid* unless there is a specific lawful basis for such processing.[19] This categorical approach has been a basic principle of EU privacy law since the Data Protection Directive was passed in 1995 and is expanded under the EU's new overarching privacy law, the General Data Protection Regulation (GDPR), which will go into effect on May 25, 2018. This "banned unless proven otherwise" principle includes the use of algorithmic agents, which are not permitted under the GDPR except under certain conditions.[20]

The Article 29 Working Party (WP29) has issued guidelines addressing algorithm profiling—what the GDPR calls "automated decision-making"—and the framework it outlines is fascinating both in its potential to fundamentally alter the way in which companies conduct online activities as well as for its divergence from US law.[21]

Profiling That Has a Legal "Similarly Significant" Effect

According to the WP29 Guidelines, "profiling" is an automated form of processing, carried out on personal data, the objective of which is to evaluate personal aspects about a natural person.[22] Generally speaking, the GDPR prohibits entities from using "solely" automated profiling to make decisions that have a legal or "similarly significant" effect on EU residents.[23] "Legal effects" are broadly defined to mean effects on people's legal rights or legal status, such as their entitlement to a social benefit granted by law, their ability to enter at the border, or increased security measures or surveillance by the competent authorities.[24]

A decision has a "similarly significant effect" if it has the potential to significantly influence the circumstances, behavior, or choices of such individual.[25] Examples include the automatic refusal of an online credit application or e-recruiting practices without any human intervention.[26] Online behavioral advertising may fall into this category in cases where it is intrusive or targets individuals' vulnerabilities; for example, regularly showing online gambling advertisements to individuals in financial difficulty who may then sign up for these offers and potentially incur further debt.[27]

There are exceptions to the prohibition on solely automated decision making. The GDPR permits automated processing if it is

1. necessary for entering into, or performance of, a contract between the individual and a data controller (although the WP29 makes it clear that this must be truly necessary and not just incidental to the contract);
2. permitted by EU Member State law; or
3. based on the individual's explicit consent (which the Guidelines suggest will be difficult in practice to obtain).[28]

One mechanism for avoiding the ban on solely automated processing is for companies to inject some layer of human oversight into the processing channel. The Guidelines address this possibility by clarifying that human oversight must be meaningful, and not just a token gesture. It should be carried out by someone who has access to all available data and has the authority and competence to change the decision.[29]

General Profiling

Even if the automated decision-making falls under one of the exceptions listed above, the GDPR requires the controller, at the time the data are collected, to provide the following:

1. notice to the data subject that the controller is engaging in this type of activity;
2. meaningful information about the logic involved; and
3. explanation of the significance and envisaged consequences of the processing.[30]

One of the biggest challenges for companies complying with the GDPR will be to devise language that provides meaningful information about the logic used for automated decision making without revealing proprietary or competitively sensitive information.[31]

Data controllers also will face challenges in complying with the GDPR's requirements for "data minimization" (personal data can only be collected when necessary for a stated purpose), "purpose limitation" (personal data may only be used for that purpose), and "storage limitation" (personal data may only be retained for as long as necessary to achieve the stated purpose).[32] This may entail operational adjustments for many companies.

Similarly, complying with "right to access" or "right to erasure" requests may require that companies engaging in automated decision-making operations develop user-accessible ways to access, review, and correct data collected about them.

Due to the inherent risk of error or bias in automated decision making, WP29 notes that a data protection impact assessment may be warranted to assess the risks associated with the processing. Special consideration must be given when engaging in profiling or automated decision making in relation to children, who are a more vulnerable segment of society.[33]

GDPR-covered entities that engage in automated decision-making should begin to reassess their practices and make the necessary changes as soon as possible. U.S companies in particular should carefully analyze and document their decisions concerning profiling activities, which, for many, will be a time-consuming and ongoing process.

Conclusion

The US and EU legal responses discussed above represent two very different jurisprudential approaches toward the complex web of legal issues raised by algorithmic profiling. The US response to the poorly understood but ubiquitous use of algorithms for online commerce reflects a laissez-faire belief that technology should be allowed to develop up to the point at which it manifests clearly defined legal harms.

On the other hand, the EU, through the GDPR, has chosen a highly complex, categorical approach toward regulating privacy in general, and algorithmic processing in particular, by strictly limiting the use of such algorithms unless a specific legal justification can be documented. This approach has been variously criticized as being unduly burdensome to business, unrealistic, and the death knell

of online behavioral advertising—the lifeblood of the internet economy.[34] It remains to be seen which approach is more effective at curbing the potential, but still not clearly understood, negative effects of algorithmic agents while allowing other technological solutions to develop that may mitigate those effects. ■

Endnotes

1. Claire Cain Miller, *When Algorithms Discriminate*, N.Y. Times, July 9, 2015.
2. *Id.*
3. *Id.*
4. *Id.*
5. B. Bodo et al., *Tackling the Algorithmic Control Crisis—The Technical, Legal, and Ethical Challenges of Research into Algorithmic Agents*, 19 Yale J.L. & Tech. 133, 139 (2017) (citing Jean-Christopher Plantin et al., *Infrastructure Studies Meet Platform Studies in the Age of Google and Facebeook*, New Media & Soc. 1 (2016)).
6. *Id.*
7. *Id.*
8. *Id*. at 139–40.
9. *Id.* at 142.
10. *Id.* (citing Randall Munroe, *Reditt's New Comment Sorting Systems*, Reddit Blog (Oct. 15, 2009), https://perma.cc/N3LT-WKU3).
11. *Id.* at 144.
12. FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising (Feb. 2009), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf.
13. *Id.*
14. Digital Advertising Alliance, Self-Regulatory Principles for Online Behavioral Advertising (July 2009), http://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/seven-principles-07-01-09.pdf.
15. Cal. Bus. & Prof. Code, div. 8, §§ 22575–79.
16. *Id.*
17. *See, e.g.*, Exec. Office of the President, Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights (May 2016); Office of the Comptroller of the Currency, Supporting Responsible Innovation in the Federal Banking System: An OCC Perspective (Mar. 2016); Fed. Trade Comm'n, Big Data: A Tool for Inclusion or Exclusion? (Jan. 2016); Ctr. for Fin. Servs. Innovation, Big Data, Big Potential: Harnessing Data Technology for the Underserved Market (Mar. 2015).
18. *Id.*
19. General Data Protection Regulation, arts. 5, 6.
20. *Id.*, arts. 22, 23.
21. Art. 29 Data Prot. Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, WP251rev.01 (Feb. 2018), http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.
22. *Id.* at 6.
23. *Id.* at 20.
24. *Id.* at 21–22.
25. *Id.*
26. *Id.*
27. *Id.*
28. *Id*. at 23–24.
29. *Id*. at 21.
30. *Id.* at 25.
31. *Id.*
32. *Id.* at 26–28.
33. *Id.* at 29–30.
34. Jim Edwards, *Wall Street Is Beginning to Worry About the Effect of GDPR on Facebook*, Wall St. J. (Feb 5, 2018), http://www.businessinsider.com/wall-street-worrying-about-effect-of-gdpr-on-facebook-2018-2; Christopher Coughlan, *GDPR Compliance: Customers Will Be the Harshest Critics*, Ashfords (Jan. 22, 2018), https://www.ashfords.co.uk/news-and-events/general/gdpr-compliance-customers-will-be-the-harshest-critics/; *#GDPR: Technology Think Tank Criticizes New EU Data Regulation,* EU Reporter (Apr. 15, 2016), https://www.eureporter.co/frontpage/2016/04/15/gdpr-technology-think-thank-criticized-new-eu-data-regulation/

Communications Lawyer
Volume 33:4
Spring/Summer
2018

AMERICAN BAR ASSOCIATION
Forum on Communications Law

Officers, Governing Committee, and Editors 2017 – 2018

Chair
Carolyn Y. Forrest
Fox Television Stations, LLC

Chair-Elect
David Giles
EW Scripps Co.

Immediate Past Chair
David J. Bodney
Ballard Spahr LLP

Budget Chair
James T. Borelli

Membership Co-Chair
Robb S. Harvey
Waller Lansden Dortch & Davis, LLP

Cynthia Counts
Duane Morris LLP

Editors

Lee S. Brenner
Kelley Drye & Warren LLP

Amanda M. Leith
NBCUniversal Media LLC

Drew Shenkman
Cable News Network

ABA Staff

Forum Director
Yolanda Muhammad
Yolanda.Muhammad@americanbar.org

Designer
Cory Ottenwess
ABA Publishing

Governing Committee

Members
Lynn D. Carrillo (2019)
Kumar Ambika Doran (2018)
Rachel R. Fugate (2019)
Robb S. Harvey (2019)
Kathleen A. Kirby (2018)
Gregg Leslie (2018)
Steven P. Mandell (2020)
Judith Mercier (2018)
Nathan Siegel (2020)
Nabiha B. Syed (2020)
Regina Thomas (2018)

Program Chairs

Privacy and Data Security CLE Program Chair
S. Jenell Trigg
Lerman Senter PLLC

Representing Your Local Broadcaster Program Chair
Kathleen Kirby
Wiley Rein LLP

Division Co-chairs

Eastern
Stephanie Abrutyn
Shaina Ward
Lee R. Williams

Central
Karen Flax
Natalie J. Spears
Leita Walker

Western
Lisa Rafferty
Elizabeth Ryder
Steven D. Zansberg