2016 SUPPLEMENT

to

MEDIA AND THE LAW

Second Edition

David Kohler
Lee Levine
David Ardia
Dale Cohen
Mary-Rose Papandrea

Carolina Academic Press
700 Kent Street
Durham, North Carolina 27701
Telephone (919) 489-7486
Fax (919) 493-5668
www.cap-press.com

TABLE OF CONTENTS

CHAPTER 1: DEFINING AND REPRESENTING THE MEDIA....3

CHAPTER 2: FIRST AMENDMENT PROTECTIONS....4

CHAPTER 3: PRIOR RESTRAINTS....6

CHAPTER 4: DEFAMATION....8

CHAPTER 5: PRIVACY....15

CHAPTER 7: INTELLECTUAL PROPERTY....23

CHAPTER 8: CIVIL AND CRIMINAL LIABILITY....24

CHAPTER 9: INDIRECT RESTRAINTS....34

CHAPTER 10: ACCESS TO INFORMATION....36

CHAPTER 11: GOVERNMENT REGULATION OF ELECTRONIC MEDIA....38

CHAPTER 1: DEFINING AND REPRESENTING THE MEDIA

Page 25, after Note 2:

3. A recent Harvard Law Review essay discusses the role of lawyers in our evolving media environment. Marvin Ammori, *The "New"* New York Times*: Free Speech Lawyering in the Age of Google and Twitter*, 127 HARV. L. REV. 2259 (2014). Professor Ammori argues that while lawyers at the leading national newspapers historically have shaped the freedom of expression, increasingly lawyers at top technology companies like Google, Twitter, and Facebook are taking on that role.

CHAPTER 2: FIRST AMENDMENT PROTECTIONS

Page 132, at the end of Note 1:

In *Jordan v. Jewel Food Stores, Inc.*, 743 F.3d 509 (7th Cir. 2014), retired basketball player Michael Jordan brought a right of publicity and trademark claims against a supermarket chain for publishing a full-page advertisement in a commemorative issue of *Sports Illustrated* dedicated to Jordan's career on the occasion of his induction into the Basketball Hall of Fame. The ad pictured a pair of sneakers labeled with Jordan's number 23, the Jewel logo, and the following text:

> A Shoe In!
>
> After six NBA championships, scores of rewritten record books and numerous buzzer beaters, Michael Jordan's elevation in the Basketball Hall of Fame was never in doubt! Jewel–Osco salutes # 23 on his many accomplishments as we honor a fellow Chicagoan who was "just around the corner" for so many years.

[You can view the advertisement in the Appendix to the court's opinion.] The text plays off of Jewel's slogan that "Good things are just around the corner."

The Seventh Circuit held that the advertisement was commercial speech even though it did not "propose a commercial transaction." Citing *Bolger*, the court concluded that "[t]he notion that an advertisement counts as 'commercial' only if it makes an appeal to purchase a particular product makes no sense today, and we doubt that it ever did," especially given the prevalence of often creative and sometimes subtle brand-awareness advertising. Taking into account the prominence of the defendant's logo in the ad and the incorporation of its slogan into its text, the court concluded that the advertisement "has an unmistakable commercial function: enhancing the Jewel-Osco brand in the minds of consumers." In reaching its holding, the court expressed concerns that a contrary ruling "would have sweeping and troublesome implications for athletes, actors, celebrities, and other trademark holders seeking to protect the use of their identities or marks." At the same time, the court emphasized that its decision is limited to the particular facts of the case: "Nothing we say here is meant to suggest that a company cannot use its graphic logo or slogan in an otherwise noncommercial way without thereby transforming the communication into commercial speech."

Page 132, after Note 3:

4. As you should recall from *Citizens United v. FECC* [see page 94-98], the Supreme Court has made clear that the First Amendment protects corporate speech. The commercial speech doctrine does not operate to limit the speech rights of corporations generally; it limits only the commercial speech (however defined) of those corporations. A recent empirical analysis of First Amendment cases suggests that in recent years, corporations are increasingly displacing individuals as the beneficiaries of First

Amendment protection. *See* John C. Coates IV, *Corporate Speech and the First Amendment: History, Data, and Implications*, 30 CONST. COMMENT. 223 (2015).

CHAPTER 3: PRIOR RESTRAINTS

Page 196, after Note 3:

4. The Supreme Court of Texas has upheld a court order requiring a defendant to remove from its website speech determined to be defamatory at a trial on the merits. *See* Kinney v. Barnes, 443 S.W.3d 87 (Tex. 2014), *cert. denied*, 135 S. Ct. 1164 (2015). The court held that such an injunction is not a prior restraint but rather is more "accurately characterized as a remedy for one's abuse of the liberty to speak." The court explained that "[s]uch an injunction does not prohibit future speech, but instead effectively requires the erasure of past speech that has already been found to be unprotected in the context in which it was made." The court "express[ed] no opinion" on the constitutionality of an injunction requiring a defendant to ask third parties to remove content from websites over which the defendant lacks control.

Notably, *Kinney* rejected the plaintiff's request for an injunction barring the defendant from making statements similar to the libelous statements in the future. Agreeing with dissenting California Supreme Court Justice Kennard in *Balboa Island Village Inn v. Lemen* [included in the casebook at pages 187-92], the Texas Supreme Court held that any injunction on future speech would be "necessarily ineffective, overbroad, or both." The court explained that a narrow injunction would "only invite the defamer to engage in word play," while a broader injunction would inevitably be overbroad given the contextual nature of the defamation tort.

The Seventh Circuit has expressly declined, for the moment, to determine "whether it is ever proper to enjoin speech." McCarthy v. Fuller, 810 F.3d 456 (7th Cir. 2015). Faced with a plainly overbroad permanent injunction that required the defendant to take down his entire website, the court remanded the case for reconsideration. Judge Posner, writing for the majority, expressed concern that a rule prohibiting all injunctions of libelous speech "would make an impecunious defamer undeterrable," but at the same time noted that it is important to keep in mind that "[a]n injunction against speech harms not just the speakers but also the listeners (in this case the viewers and readers)" by interfering with their right to receive information.

Page 210, after Note 2:

3. In January 2016, famous British singer Elton John and his husband, David Furnish, obtained a preliminary injunction preventing any British or Welsh news outlet from reporting on names and details surrounding their relationship. News had just surfaced that Mr. Furnish had cheated on Elton John multiple times, and the couple successfully enjoined publishers from writing about the affair. The United Kingdom's Supreme Court affirmed the injunction. The court found that the couple still had a right to privacy, even though the names and details of the affair had been released on the Internet. The court concluded that restraining the publication of the information despite its widespread publication in social media would protect the plaintiff's privacy interests from greater erosion. Perhaps even more remarkably, the court concluded the injunction

would help protect the plaintiffs' young children from learning this information about their parents prematurely. See PJS v. News Group Newspapers Ltd., [2016] UKSC 26, [2016] EWCA Civ 393, [36] (appeal taken from Eng.).

CHAPTER 4: DEFAMATION

Page 226, third paragraph:

There have been some important recent developments regarding the constitutionality of anti-SLAPP statutes as well as their applicability in federal courts.

"SLAPP" stands for "strategic litigation against public participation." Anti-SLAPP statutes developed as a means of terminating lawsuits that chill discussions of public issues. Such lawsuits, it is contended, are never intended to be successful but rather are filed as a means of intimating speakers by forcing them to endure the expense, emotional toll, and potential risk of litigation. The concern is that speakers will quickly settle such lawsuits rather than defend their First Amendment rights.

Although the details of anti-SLAPP statutes vary from state to state, they all generally permit a qualifying defendant to file a special motion to strike a plaintiff's claim. The plaintiff bears the burden of demonstrating a probability of success. While the motion is pending, discovery is stayed unless the plaintiff demonstrates "good cause" for limited discovery to meet its burden. If an anti-SLAPP motion is granted, a defendant is entitled to obtain not just the dismissal of claims but also the recovery of moving costs, attorneys' fees, and at times statutory damages and other relief the court deems necessary to deter similar conduct in the future. SLAPP statutes have been increasingly invoked in defamation actions, including by media defendants, to secure the early dismissal of such cases, often without the need for costly discovery.

A circuit split has developed on the question of whether the application of state anti-SLAPP laws by federal courts sitting in diversity violates the *Erie* doctrine because they conflict with the Federal Rules of Civil Procedure. Some courts have held that federal courts cannot apply state anti-SLAPP statutes because the state laws conflict with the procedures for the early dismissal of cases under Rules 12 and 56. *See*, *e.g.*, Abbas v. Foreign Policy Group, LLC, 783 F.3d 1328 (D.C. Cir. 2015). The Eleventh Circuit has held that Georgia's anti-SLAPP statute, which requires plaintiffs and their attorneys to file a verification that their complaints are made in good faith and without an improper purpose, does not apply in federal court because it conflicts with F.R.C.P. 11. *See* Royalty Network Inc. v. Harris, 756 F. 3d 1351 (11th Cir. 2014). Other courts have rejected *Erie*-doctrine challenges, holding that federal courts can apply anti-SLAPP statutes because the state laws merely supplement the federal rules and/or do not conflict with them. *See*, *e.g.*, Godin v. Schencks, 629 F.3d 79 (1st Cir. 2010); Henry v. Lake Charles American Press, L.L.C., 566 F.3d 164 (5th Cir. 2009); United States ex rel. Newsham v. Lockheed Missiles & Space Co., 190 F.3d 963 (9th Cir. 1999). The Supreme Court has so far declined to resolve the issue. *See, e.g.*, Mebo Intern., Inc. v. Yamanaka, 136 S. Ct. 1449 (2016) (denying petition for writ of certiorari).

In addition, the Supreme Court of Washington has held that its state's anti-SLAPP statute is unconstitutional because it violates the constitutional right to trial by jury. *See* Davis v. Cox, 183 Wash.2d 269, 351 P.3d 862 (2015).

Page 278, after Note 4:

5. In *Milkovich*, the Supreme Court took great pains to make clear that couching statements in terms of opinion using phrases such as "I believe" or "I think" do not categorically immunize a speaker from defamation actions. *Milkovich* specifically explained that "the statement, 'In my opinion Jones is a liar,' can cause as much damage to reputation as the statement, 'Jones is a liar.'" The discussion of the difference between fact and opinion in the securities regulation case *Omnicare, Inc. v. Laborers Dis. Council Const. Industry Pension Fund*, 135 S. Ct. 1318 (2015), appears to be inconsistent with *Milkovich*.

Section 11 of the Securities Act of 1933 requires any company that wants to sell securities in interstate commerce to file a registration statement with the Securities and Exchange Commission. Purchasers of the securities can sue if the registration statement contains either "an untrue statement of material fact" or "omit[s] a material fact . . . necessary to make the statements not misleading." Omnicare's registration statement declared that the company "believe[d]" that its various contracts with other healthcare providers and pharmaceutical manufacturers and sellers were compliant with state and federal laws. After the federal government sued Omnicare for entering into illegal kickback agreements with pharmaceutical manufacturers, various pension funds sued the company, arguing that its registration contained "untrue statements of material fact." Justice Kagan, writing for the Court, held that the challenged statements did not contain an "untrue statement of material fact."

> As the Funds put the point, a statement of belief may make an implicit assertion about the belief's "subject matter": To say "we believe X is true" is often to indicate that "X is in fact true." In just that way, the Funds conclude, an issuer's statement that "we believe we are following the law" conveys that "we in fact are following the law"—which is "materially false," no matter what the issuer thinks, if instead it is violating an anti-kickback statute.
>
> But that argument wrongly conflates facts and opinions. A fact is "a thing done or existing" or "[a]n actual happening." WEBSTER'S NEW INTERNATIONAL DICTIONARY 782 (1927). An opinion is "a belief[,] a view," or a "sentiment which the mind forms of persons or things." Most important, a statement of fact ("the coffee is hot") expresses certainty about a thing, whereas a statement of opinion ("I think the coffee is hot") does not. See *ibid.* ("An opinion, in ordinary usage ... does not imply ... definiteness ... or certainty"); 7 OXFORD ENGLISH DICTIONARY 151 (1933) (an opinion "rests[s] on grounds insufficient for complete demonstration"). Indeed, that difference between the two is so ingrained in our everyday ways of speaking and thinking as to make resort to old dictionaries seem a mite silly. And Congress effectively incorporated just that distinction in § 11's first part by exposing issuers to liability not for "untrue statement[s]" full stop (which would have included ones of opinion), but only for "untrue statement[s] of ... *fact*."

> The two sentences to which the Funds object are pure statements of opinion: To simplify their content only a bit, Omnicare said in each that "we believe we are obeying the law." And the Funds do not contest that Omnicare's opinion was honestly held. Recall that their complaint explicitly "exclude[s] and disclaim[s]" any allegation sounding in fraud or deception. What the Funds instead claim is that Omnicare's belief turned out to be wrong—that whatever the company thought, it was in fact violating anti-kickback laws. But that allegation alone will not give rise to liability under § 11's first clause because, as we have shown, a sincere statement of pure opinion is not an "untrue statement of material fact," regardless whether an investor can ultimately prove the belief wrong. That clause, limited as it is to factual statements, does not allow investors to second-guess inherently subjective and uncertain assessments. In other words, the provision is not, as the Court of Appeals and the Funds would have it, an invitation to Monday morning quarterback an issuer's opinions.

The Court ultimately remanded the case for consideration of whether Omnicare omitted material facts that rendered its statements misleading.

Although the Court did not cite or otherwise acknowledge *Milkovich*, "the opinion's expansive treatment of fact and opinion actually have much to offer in defamation defense matters." Cynthia L. Counts & Kenneth Argentieri, *Demystifying the Law of Opinion and Embracing Milkovich*, 32-WTR COMM. LAW. 15 (Winter, 2016).

Page 288, after *Masson v. New Yorker Magazine, Inc.*:

In *Air Wisconsin Corps. v. Hoeper*, 134 S. Ct. 852 (2014), the Supreme Court expanded on how courts should determine whether allegedly defamatory statements are "materially false." The case concerned the interpretation of the Aviation and Transportation Security Act (ATSA), which provides protection to airlines and their employees who report security threats. The Act specifically provides that the immunity does not apply to "any disclosure made with actual knowledge that the disclosure was false, inaccurate, or misleading" or "any disclosure made with reckless disregard as to the truth or falsity of that disclosure." The Court explained that the immunity provisions of that law were patterned after *New York Times v. Sullivan* and accordingly incorporated *Masson*'s materiality requirement. The Court explained in determining whether allegedly defamatory statements "would have a different effect on the mind of the reader [or listener] from that which the . . . truth would have produced," courts must take into account that "the identity of the relevant reader or listener varies according to the context."

In this case, the Court considered the perspective of a "reasonable security officer." The Court made clear that the inquiry was an objective one and did not focus on the

actual significance of the challenged statements to a particular security official. Although the materiality inquiry in defamation claims is aimed at determining whether the plaintiffs' reputation has been harmed, the Court explained, the materiality requirement inherent in the ATSA immunity inquiry is concerned with "whether a falsehood affects the authorities' perception of and response to a given threat." The Court concluded as a matter of law the challenged statements in this case where not materially false.

Specifically, airline official Patrick Doyle called TSA after the plaintiff had an outburst after failing a flight simulator test he needed to pass to retain his job and made the following three statements that were the basis for the plaintiff's defamation claims:

Statement 1: Plaintiff was a Federal Flight Deck Officer (FFDO) who "may be armed."

> The Court held that this statement was literally true – he was an FFDO, and he had been issued a weapon – and rejected the plaintiff's contention that LaWare should have clarified that he had no specific reason to believe he was actually armed at that time. Any confusion about whether he was actually carrying his gun was "immaterial" because "[a] reasonable TSA officer, having been told only that Hoeper was an FFDO and that he was upset about losing his job, would have wanted to investigate whether Hoeper was carrying his gun."

Statement 2: Plaintiff "was terminated today."

> Although the plaintiff was not fired until the day after this statement was made, the Court reasoned that the statement was not materially false because the plaintiff's behavior made it clear that he would be fired imminently. The Court concluded that "[n]o reasonable TSA officer would care whether an angry, potentially armed airline employee had just been fired or merely knew he was about to meet that fate."

Statement 3: The pilot was "[u]nstable" and that it was "concerned about his mental stability."

> The Court first held that "from the perspective of a reasonable security officer, there is any material difference between a statement that the plaintiff had just 'blown up' in a professional setting and a statement that he was '[u]nstable.'" The Court then held that although some airline officials testified that they would not have chosen those precise words did not undermine ATSA immunity because this statement "accurately conveyed 'the gist' of the situation; it is irrelevant whether trained lawyers or judges might with the luxury of time have chosen more precise words."

Justice Scalia, joined by Justices Thomas and Kagan, concurred that the materiality standard applied but dissented on the application of that standard in this case. Scalia argued that a jury *could* determine that the plaintiff's behavior at the flight simulator test was nothing more than a "brief, run-of-the-mill, and arguably justified display of anger" that would not lead anyone present to regard him as irrational or potentially violent.

Justice Scalia criticized the majority as failing to respect "the wisdom of preserving the jury's role in this inquiry, designed to inject a practical sense that judges sometimes lack."

Commentators have suggested that the Court's emphasis on the audience may lead to the early dismissal of some defamation claims, particularly given the increasing numbers of new media communications aimed at "niche" communities. *See* Charles D. Tobin & Len Niehoff, *Material Falsity in Defamation Cases: The Supreme Court's Call for Contextual Analysis*, 30-JUN COMM. LAW. 9 (June 2014).

Indeed, in recent years courts have increasingly paid attention to the particular audience for challenged statements when determining whether those statements are capable of defamatory meaning.

Page 394, after Note 1:

Under what conditions a website loses its immunity for third-party content has been the subject of state and federal court decisions in that last two years.

In a widely anticipated decision, the Sixth Circuit held that the website Dirty.com was entitled to Section 230 immunity from defamation claims brought by a teacher and former cheerleader for the Cincinnati Bengals professional football team who was the subject of several unwelcome comments about her submitted by anonymous users of the site. Jones v Dirty World Entertainment Records, LLC, 755 F.3d 398 (6th Cir. 2014). Dirty.com encourages users to upload "dirt" – content including text, photographs, or videos of any subject. The website owner and his staff decide which material to post and makes brief editorial comments about it, but they do not materially change, create, or modify any of the user-submitted material.

The federal district court had held that "a website owner who intentionally encourages illegal or actionable third-party postings to which he adds his own comments ratifying or adopting the posts becomes a 'creator' or 'developer' of that content and is not entitled to immunity." The Sixth Circuit rejected this "encouragement" test, explaining that such a test "would inflate the meaning of 'development' [in Section 230] to the point of eclipsing the immunity from publisher-liability that Congress established. Many websites not only allow but also actively invite and encourage users to post particular types of content." The Sixth Circuit added that websites do not lose immunity from lawsuits based on third-party content simply by selecting third-party content for publication or by commenting on that content when the comments are not themselves defamatory. Furthermore, and perhaps most significantly, the court explained that "[u]nlike in *Roommates.com*, [the Dirty.com] did not require users to post illegal or actionable content as a condition of use."

Other courts have been more willing to reject Section 230 defenses, at least at the motion to dismiss stage, in cases where plaintiffs have alleged that the defendant website was not "neutral" about the content third parties posted. Perhaps the most significant decision taking this approach in recent years is *J.S. v. Backpage.com*, 184 Wash.2d 95

(Wash. 2015) (en banc), which rejected a website's Section 230 immunity claim in a case involving third-party advertisements for sexual services. The court held that the plaintiffs' allegations that Backpage.com designed its advertising posting rules in such a way to help pimps evade law enforcement was enough to defeat Section 230 immunity, at least at that early stage of the litigation. The court reasoned the plaintiff had adequately alleged that "Backpage's advertising rules were not simply neutral policies prohibiting or limiting certain content but were instead specifically designed . . . so that pimps can continue to use Backpage.com to traffic in sex." In contrast, the U.S. Court of Appeals for the First Circuit held that Backpage,com is entitled to Section 230's protections at the motion to dismiss stage, notwithstanding similar allegations that its advertising policies encourage sex trafficking advertisements. Jane Doe No. 1 v. Backpage.com, LLC, 817 F.3d 12 (1st Cir. 2016) (holding that "claims that a website facilitates illegal conduct through its posting rules necessarily treat the website as a publisher or speaker of content provided by third parties and, thus, are precluded by section 230(c)(1)").

Similarly, websites that encourage users to post reviews of businesses or other service providers have met with mixed success when asserting Section 230 immunity. For example, a federal district court in Utah held that the owner of the website Ripoff Report was not entitled to Section 230 immunity. Relying in part on *Roommates.com*, the court explained that an internet service provider is sufficiently "responsible" for the development of content posted by a third party if it is not "neutral" with respect to the offensiveness of that content. The court accepted the plaintiff's allegations that Ripoff Report encouraged negative reviews. *See* Vision Security, LLC v. Xcentric Ventures, Case. No. 2:13-CV-00926 (Aug. 27, 2015 C.D. Utah).

Page 394, at end of Note 3:

5. Plaintiffs have continued to attempt to bypass Section 230 immunity by asserting claims that do not directly rely on the content of material on a website, and these attempts have been successful in some instances. The most significant of these decisions comes from the U.S. Court of Appeals for the Ninth Circuit, which has permitted a lawsuit to go forward against modelmayhem.com, a model networking site, for allegedly failing to warn users that two individuals had been browsing the website to lure women to fake modeling auditions where they would instead be drugged, raped, and filmed for a pornographic video. In *Doe 14 v. Internet Brands, Inc.*, No. 12-56638, 2016 WL 3067995 (9th Cir. May 31, 2016), the Ninth Circuit rejected the defendant's motion to dismiss the case under Section 230 because the plaintiff did not seek to hold the website liable for any of its content but rather on the theory that the website had a "special relationship" with its users giving rise to a duty to warn. The court explained that the claim did not seek to hold Internet Brands liable as a "publisher or speaker" because this failure to warn claim "would not require Internet Brands to remove any user content or otherwise affect how it publishers or monitors such content." The claims against the website were not based on its failure to remove content from the website but rather for its failure to tell its users that it had information that third parties were using the website to target victims.

In contrast, the D.C. Circuit has rejected the argument that social media websites have a special relationship with their users giving rise to a heightened state-law duty of care that would support a non-preempted tort claim. *See* Klayman v. Zuckerberg, 753 F.3d 1354 (D.C. Cir. 2014) (granting motion to dismiss negligence and intentional assault claims against Facebook based on allegations the social media site permitted the publication of a webpage urging Muslims to kill Jewish people), *cert denied*, 135 S. Ct. 680 (2014).

6. Other courts have limited Section 230 immunity in cases where plaintiffs have alleged that defendants failed to make filtering decisions in good faith. Section 230(c)(2) provides immunity for "any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable…." For example, in *e-ventures Worldwide, LLC v. Google*, 2016 WL 2758889 (M.D. Fla. May 12, 2016), a district court held that Google was not entitled to Section 230 immunity at the motion to dismiss stage where the plaintiff alleged Google had removed links to the plaintiff's websites from Google's search results for anticompetitive and punitive purposes—in other words, in bad faith.

CHAPTER 5: PRIVACY

Page 459, at end of Note 7:

Update on *Bollea v. Gawker Media* litigation: After the federal district court rejected Terry Gene Bollea's motion for preliminary injunctive relief, Bollea voluntarily dismissed his federal case and refiled it in Florida state court, where he essentially made the same claims he had made in federal court. Bollea again filed a motion for a temporary restraining order (TRO). The state trial court granted his motion, but without making any findings supporting its decision at the hearing or in the written order of its decision. The defendants appealed the injunction to the state appellate court, which reversed, holding that Bollea had "failed to meet the heavy burden of overcoming the presumption that the [TRO] is invalid as an unconstitutional prior restraint in violation of the First Amendment." Gawker Media, LLC v. Bollea, 129 So.3d 1196 (Fla. 2d. DCA 2014). The appellate court noted that in *Michaels I* [mentioned in the current Note 7], the defendants published the sex tape at issue for solely commercial purposes, while in *Bollea*, "the written report and video excerpts are linked to a matter of public concern—Mr. Bollea's extramarital affair and the video evidence of such—as there was ongoing public discussion about the affair and the Sex Tape, including by Mr. Bollea himself."

After remand, the case went to trial, and a Florida jury awarded Bollea $140 million. Gawker's appeal is pending. After the jury verdict came down, Silicon Valley billionaire Peter Thiel revealed that he had funded Bollea's lawsuit against Gawker, as well as others. See Andrew Ross Sorkin, *Peter Thiel, Tech Billionaire, Reveals Secret War with Gawker* (N.Y. TIMES May 25, 2016).

Page 459, Note 8:

As of July 2016, thirty-four states plus the District of Columbia have passed laws criminalizing the dissemination of revenge porn. All the individual laws each prohibit the disclosure or dissemination of naked photographs or videos of another person without that person's consent. The precise terms of these statutes vary from state to state, but some trends are apparent. Most states require some legitimate expectation of privacy, thereby excluding photographs or videos of public nudity. Many states require the perpetrator to have intended to harm or distress the victim, and nine states even require the victim to be actually distressed. Colorado exempts depictions that are "newsworthy," while many other states exempt disclosures that were made with a lawful or legitimate purpose. COLO. REV. STAT. § 18-7-107 (2015).

Many state revenge porn statutes also include exceptions for interactive computer services or other internet providers, in keeping with Section 230 protections. But at least one court has concluded that Section 230 does not always protect websites that encourage users to post revenge porn. *See* California v. Bollaert, 248 Cal.App.4th 699 (Cal. Ct. App. 2016). The *Bollaert* defendant ran the revenge porn website UGotPosted, which accepted submissions of private, intimate photographs along with the person's personal information and Facebook profile. Relying on *Roommates.com*, the California Court of Appeals determined that a website does not receive CDA immunity if it is intentionally

designed to require users to post illegal or actionable content as a condition of use, and UGotPosted required users to violate a person's privacy in order to upload pictures.

Page 502, after Note 3:

4. Keep in mind that a plaintiff's ability to recover for invasions of privacy are greatly impacted by relevant state statutory or common law. For example, as *Jews for Jesus, Inc. v. Rapp* [see pages 475-81] demonstrates, not all States recognize a false light privacy claim. Likewise, some states do not recognize publication of private facts claims. *See*, *e.g.*, Hall v. Post, 372 S.E.2d 711 (N.C. 1988) (holding the publication of private facts tort does not exist in North Carolina because recognizing such a tort "would add to the existing tensions between the First Amendment and the law of torts and would be of little practical value to anyone").

A recent case illustrates the limits of New York's privacy law. In *Foster v. Svenson*, 128 A.D.3d 150 (N.Y. App. Div. 2015), a state appellate court affirmed the dismissal of privacy claims a family brought against a photographer who had secretly taken pictures of them through the windows of his own apartment into theirs. The defendant included some of these photographs in a series called "The Neighbors," which he exhibited at galleries in New York and Los Angeles. Although the defendant asserted he tried to obscure the identity of the individuals in his photos, the plaintiffs' young children were clearly identifiable.

The court explained that New York privacy law limits recovery to those whose identity is used "for advertising purposes" or "for purpose of trade." Although based on its plain language statute would appear to apply all items bought and sold in trade, court decisions have made clear that the statute is not applicable to publications involving newsworthy events and matters of public concern. [*See*, *e.g.*, Arrington v. New York Times Co., on pages 492-94.] The court held that just as the statute did not apply to works of art any more than it applied to literature, movies, and theater that satisfy the newsworthiness and public concern exemption. The court noted that this exemption could be lost if the privacy invasion is "atrocious, indecent and utterly despicable," but that the intrusion here was not sufficiently "outrageous." The court concluded that although the facts of the case were "troubling," complaints like these involving "heightened threats of privacy posed by new and ever more invasive technologies" should be directed to the New York legislature.

Page 539, after Note 4:

4. As you can see from the cases in the section on the right of publicity, it remains unclear what limits, if any, the First Amendment places on the right of publicity over and above the statutory and common law limits of such rights. One lurking question is whether it is constitutionally relevant that the challenged expression is commercial or noncommercial speech. (See Chapter 2 for a discussion of the reduced constitutional protections for commercial speech.) In *Jordan v. Jewel Food Stores, Inc.*, 743 F.3d 509 (7th Cir. 2014), discussed earlier in this Update, the plaintiff Michael Jordan did not

challenge the defendant's argument that the First Amendment bars right of publicity and trademark claims if the advertisement at issue is noncommercial speech. The Seventh Circuit remarked that "it's far from clear" whether Jordan's claims would necessarily fail if the ad constituted noncommercial speech because "[t]he Supreme Court has never addressed the question, and decisions from the lower courts are a conflicting mix of balancing tests and frameworks borrowed from other areas of free-speech doctrine." The court concluded with an almost audible sound of relief that "Jordan's litigating position allows us to sidestep this complexity."

On remand, the district court denied Jordan's motion for summary judgment on his Illinois right of publicity claim. *Jordan v. Jewel Food Stores, Inc*., 83 F. Supp. 3d 761 (N.D. Ill. 2015), and the case ultimately settled on the eve of trial. Notably, Jordan won a $8.9 million jury verdict against another supermarket chain—the now-defunct Dominick's—which had also published an advertisement congratulating Jordan in the same commemorative issue of *Sports Illustrated*. Unlike Jewel's advertisement, however, Dominick's advertisement included a $2 coupon. The Dominick's case settled while post-trial motions challenging the jury verdict were pending.

Page 539, after Note 4:

5. The Supreme Court denied the *Hart* defendants' petition for a writ of certiorari. *See* Electronic Arts v. Hart, 135 S. Ct. 43 (2014). The parties subsequently entered into a $60 million settlement, which a district court judge has approved. Associated Press, *$60 Million Settlement Approved in N.C.A.A. Video Game Lawsuit,* NY. TIMES (Jul. 17, 2015), at D5.

College basketball and football players have also sued broadcasters, athletic conferences, and licensing agencies involved in the transmission of sporting events for conspiring to use the players' names, likenesses, and images in violation of trademark, antitrust, and right of publicity laws. In *Marshall v. ESPN*, 111 F. Supp. 3d 815 (M.D. Tenn.), a federal district court dismissed these claims. The court held that under Tennessee law, the players did not have an enforceable statutory or common law right of publicity in sports broadcasts or advertisements for those broadcasts; indeed, Tennessee's right of publicity law expressly exempts sports broadcasts. Notably, the court rejected the players' attempt to argue that *Zacchini* supported their right of publicity claims because their likenesses were used in the broadcast of entire games, rather than in brief sports reports. The court noted that unlike the players, Mr. Zacchini was both the performer and the producer of his human cannonball act. The court concluded that "[i]t is a mistake . . . to read *Zacchini* as supporting a right of publicity by anyone who performs in an event produced by someone else." Because the players had no right of publicity claims, the court held their Sherman Act claims must fail. The court also rejected the players' Lanham Act claims on the grounds that the sports broadcasts were noncommercial speech, and that in any event the use of the players' images in advertisements for the sports broadcast did not create a likelihood of confusion. The case is currently on appeal before the Sixth Circuit.

Relatedly, former professional football players brought class action lawsuit against the NFL, alleging that the league's use of video footage of the athletes in various televised productions violated their right of publicity rights. Nearly 25,000 members of the class entered into a complex settlement with the NFL; the settlement essentially set up a licensing agency to assist the ex-players with their publicity rights and required the NFL to contribute up to $43 million to a fund to assist former players. Six players objected to the settlement, but the Eighth Circuit upheld it on appeal. Marshall v. National Football League, 787 F.3d 502 (8th Cir. 2014). While the settlement was before the Eighth Circuit, the district court granted a motion to dismiss the claims of the few players who had opted out of the settlement. *See* Dryer v. National Football League, 55 F. Supp. 3d 1181 (D. Minn. 2014), *appeal filed*, No. 14-3428 (8th Cir. Oct. 28, 2014).

6. The right of publicity also arises in the context of other expressive works like books, movies, and television. In *Sarver v. Chartier*, 813 F.3d 891 (9th Cir. 2016), an Army sergeant claimed a fictional character in the awarding-winning film *The Hurt Locker* was based on his life and experiences. He brought claims for misappropriation of his right of publicity, defamation, and intentional infliction of distress against the screenwriter, producer, and director based on his claims that he did not consent to the use of his identity in the movie and that the several scenes in the movie falsely portrayed him in a way that harmed his reputation. In an eagerly awaited decision, the Ninth Circuit affirmed the district court's dismissal of his claims under California's anti-SLAPP statute. The court rejected his right of publicity claim with the following analysis:

> First, *The Hurt Locker* is not speech proposing a commercial transaction. Accordingly, our precedents relying on the lesser protection afforded to commercial speech are inapposite. Second, and critically, unlike the plaintiffs in *Zacchini, Hilton,* and *Keller,* Sarver did not "make the investment required to produce a performance of interest to the public," or invest time and money to build up economic value in a marketable performance or identity. Rather, Sarver is a private person who lived his life and worked his job. Indeed, while Sarver's life and story may have proven to be of public interest, Sarver has expressly disavowed the notion that he sought to attract public attention to himself. Neither the journalist who initially told Sarver's story nor the movie that brought the story to life stole Sarver's "entire act" or otherwise exploited the economic value of any performance or persona he had worked to develop. The state has no interest in giving Sarver an economic incentive to live his life as he otherwise would.
>
> In sum, *The Hurt Locker* is speech that is fully protected by the First Amendment, which safeguards the storytellers and artists who take the raw materials of life—including the stories of real individuals, ordinary or extraordinary—and transform them into art, be it articles, books, movies, or plays. If California's right of publicity law applies in this case, it is simply a content-based speech restriction. As such, it is presumptively unconstitutional, and cannot stand unless Sarver can show a compelling state interest in preventing the defendants' speech. Because Sarver cannot do so, applying California's right of publicity in this case would violate the First Amendment.

This reasoning of this decision is somewhat unsatisfactory for several reasons. Despite Saver's suggestion to the contrary, the right of publicity has never been limited to the use of a plaintiff's identity in commercial works. The court also fails to explain why it appears to be treating movies differently from video games. Finally, the court indicates that it might have reached a different result if the plaintiff were a public figure, but it not clear why that should be determinative. Using plaintiff's identity in *The Hurt Locker* was presumptively of some value to the defendants, and by rejecting plaintiff's right of publicity claims, the court has deprived him – and future plaintiffs – of valuable compensation.

Page 562, after "Notes and Questions":

In May 2014, the European Court of Justice held that search engines like Google must remove links to online information that is "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed and in the light of the time that has elapsed." *See* Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* [2014] CJEU (May 13, 2014). Although this new ruling is commonly called "the right to be forgotten," it might more accurately be characterized as "the right to be de-linked." Information is not removed from the web – notably the newspaper was not required to remove information about the foreclosure from its website – but search engines like Google are required to make sure certain types of information do not appear in search results.

In the CJEU case first recognizing the right to be forgotten, Mario Costeja González asked the Spanish newspaper *La Vanguardia Ediciones SL* to remove from the web stories about the foreclosure of his home, and for Google to remove these stories from search results for his name. The Court of Justice of European Union rejected the claims against the newspaper but upheld the claims against Google. This means that while information about the foreclosure is still available on the newspaper's website, a link to that article will not show up in a search result for "Mario Costeja González." In reaching this decision, the CJEU discounted the impact the right to be forgotten would have on the freedom of expression rights of the original content providers.

The CJEU decision does not require search engines to take affirmative action; instead, they are required to alter search results only if a removal request is made. That said, the court's opinion did not address precisely when search engines are required to take down information or logistically how that would be accomplished. Notably, complainants are not required to demonstrate any of the following: that the information is false or inaccurate; that the posting of the information on the website where the search engine found it was unlawful at the time or posting or had somehow become unlawful; that the appearance of the information in search results was prejudicial to the complainant; or that the information is not newsworthy or of legitimate public concern.

Google provides some information about search removal requests; for example, at last check Google reports that since May 2014 Google has evaluated over **1.6 million** URLs for removal as a result of requests from over **509**,000 people. *See* Transparency Report,

http://www.google.com/transparencyreport/removals/europeprivacy/?hl=en-US (last accessed August 4, 2016). The Guardian reports that based on its analysis of source data hidden in Google's report, 95% of requests came from private individuals seeking the removal of private information (at least according to Google's attempts to characterize the requests). Sylvia Tippman & Julia Powles, *Google Accidentally Reveals Data on "Right to be Forgotten" Requests*, THE GUARDIAN (Jul. 14, 2015), http://www.theguardian.com/technology/2015/jul/14/google-accidentally-reveals-right-to-be-forgotten-requests.

In guidelines released in November 2015, European data regulators criticized the use of statements on search results notifying users that some results had been delisted as well as the media's practice of reporting what stories had been delinked. In addition, the regulators called for Google to censor search results on Google.com as well as the country-specific website (such as Google.fr) in order to make the right to be forgotten more meaningful and effective. *See* Article 29 Working Party's Guidelines on the Implementation of the Ruling (Nov. 26, 2014), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf. In June 2015, the French data protection authority CNIL (*Commission nationale de l'informatique et des libertés*) has asked Google to scrub its search results worldwide. Google appealed this order, arguing not only that 97% of all European searches currently conducted through country-specific versions of Google (such as Google.fr), but also that, as a matter of principle, no one country should be able to dictate Internet standards for the world. Google faces potential sanctions for its refusal to comply with CNIL's request. *See* David Meyer, *Google Contests Global "Right to be Forgotten" Order*, POLITICO.COM (July 15, 2015), http://www.politico.eu/article/google-challenges-global-right-to-be-forgotten-order/.

Google's appeal was rejected, but the company found a way to comply with the EU's decision while still providing the same search results around the world. If someone accesses Google.com from a EU IP address, the search will not return URL addresses that have been blocked. However, Google.com will still return the same search results if accessed from a computer in the United States or elsewhere. This protocol allows Google to comply with EU rulings on the right to be forgotten while still maintaining their independence and integrity where such a right has not been recognized. *See* Peter Fleischer, *Adapting our approach to the European right to be forgotten*, GOOGLE EUROPE BLOG (March 4, 2016), http://googlepolicyeurope.blogspot.co.uk/2016/03/adapting-our-approach-to-european-right.html. This is not a perfect solution, however, as European residents will still be able to access blocked Google results by using virtual private networks (VPN's), similar to those used by Chinese residents to access blocked websites.

There is no right to be forgotten in the United States, and efforts to legislate one would face many potential constitutional and statutory hurdles, given the strong First Amendment protection for the publication of lawfully obtained information, as discussed earlier in Chapter 5, and the broad immunity given internet service providers in Section 230 of the Communications Decency Act (discussed in Chapter 4).

That said, limited statutory efforts intended to give individuals the right to control the dissemination of information do exist in the United States. Perhaps the most notable is California's new so-called "Eraser" Law, which requires websites and mobile applications to permit minors who are registered users to request and obtain the removal of content or information the minor user posted. CAL. ANN. BUS. & PROF. CODE § 22581 (2015). Unlike the right to be forgotten, minors are not required to make any showing regarding the value (or lack thereof) of the information for the public. But the statute is much more limited than the EU right to be forgotten. The California law does not apply to material posted by another person; it permits websites and mobile application to retain the information on its servers as long as it is not visible to users; and operators can keep the information visible if they "anonymize" it. Finally, the law appears to give the take-down right to minors only, which arguably limits its utility: adults who regret what they posted while minors would not be entitled to make removal requests. To date, no legal challenges to this law have been made, but many have noted that the law provides a right that most websites already provide their users.

Many states have criminal record erasure laws, but courts have held that such laws do not provide individuals with a right to force websites to remove truthful information have largely been unsuccessful. In one case, for example, the Second Circuit held that a plaintiff could not bring defamation claims against an online publication that accurately reported the plaintiff's arrest but did not take down the information when the charges against her were later nolled (dismissed without prejudice to refiling). The plaintiff cited Connecticut's Criminal Record Erasure statute to support her claim that the defendant had a duty to delete statements regarding her arrest. Rebuffing this argument, the Second Circuit explained that the limited purposes of criminal record erasure statutes are to prevent the government from relying on the criminal record in future proceedings and to permit defendants to deny that they have ever been arrested on job applications and in other contexts; they do not create a duty on third parties to cleanse their records. The court declared that "[t]he statute creates legal fictions, but it does not and cannot undo historical facts or convert once-true facts into falsehoods." The Second Circuit also rejected the plaintiff's defamation by implication claim because the report that the plaintiff was arrested and criminally charged is true," and "[r]easonable readers" will appreciate that some people who are arrested are not guilty or will have the charges against them dropped. Martin v. Hearst Corp., 777 F.3d 546 (2d Cir. 2015), *cert. denied*, 136 S.Ct. 40 (2015).

Recent years have seen the rise of websites that collect mug shots from public records, post them online, and charge fees to those individuals who want to have their photographs taken down. *See* David Segal, *Mugged by a Mugshot Online*, N.Y. TIMES at BU1 (Oct. 5, 2013). In reaction, several states no longer post booking photographs online; in some instances, mugshots are available through public record requests only to those who agree not to post them on websites offering to remove mug shots for a fee.

Notably, a federal district court in Pennsylvania rejected a motion to dismiss a false light claim against a mugshot website. *See* Taha v. Bucks County, 9 F. Supp. 3d 490 (E.D. Pa. 2014). The court explained that although the website contained a disclaimer

that "[a]n arrest does not mean that the individual has been convicted of the alleged violation," the overall design of the website, which included "Busted!" in large bold letters over the plaintiff's mugshot, "creates the impression that [the plaintiff] is a 'criminal' – at the very least, that he has done something wrong, that his conduct warrants monitoring in the future." The court added that "[i]f [defendant's] business model is extortion by shame, as [the plaintiff] alleges, the claim is stronger still." The court did not explain why or how the defendant's intent in publishing the arrest information about the plaintiff impacted the viability of the plaintiff's false light claim.

The court subsequently granted the website defendant's motion for summary judgment because the plaintiff could not prove the website published his mug shot with actual malice. (The plaintiff in *Taha* does not appear to be a public figure, but some lower courts apply the actual malice standard in all false light cases, or in all cases involving matters of public concern. See Note 1 on page 491.) The court explained that the website relied on the accuracy of the county website from which the mugshots were taken and believed the county had procedures in place to prevent the dissemination of expunged records. In addition, the website took down expunged records without charge, but Taha did never told the website his record had been expunged. Taha v. Bucks Cty., No. CV 12-6867, 2015 WL 9489586, at *4 (E.D. Pa. Dec. 30, 2015).

Although the First Amendment poses some challenges to legislative efforts to give people the right to control the flow of personal information, it is important to keep in mind that many Internet service providers already do give their users the ability to take down information they have posted. Intermediaries play an increasingly important role in controlling the flow of information, and these controls are not subject to constitutional limitations because the intermediaries are not state actors. With respect to extortionist mug shot websites, for example, Google have taken steps to bury such websites in search results, and payment providers have refused to process money exchanges. *See* Kashmir Hill, *Payment Providers and Google Will Kill the Mug Shot Extortion Industry Faster Than Lawmakers*, FORBES.COM (Oct. 7, 2013), http://www.forbes.com/sites/kashmirhill/2013/10/07/payment-providers-and-google-will-kill-the-mug-shot-extortion-industry-faster-than-lawmakers/ ("If we're all on board with locking up the mugshot industry, it's great. But it's also a kind of scary display of the power of private industry to control speech on the Internet."). Furthermore, Google recently announced that in addition to honoring requests to remove "highly sensitive personal information," such as social security numbers, credit card numbers, and bank account numbers, it will also honor requests from people to remove from search results nude or sexually explicit images posted online without their consent. A copy of this announcement is available at https://publicpolicy.googleblog.com/2015/06/revenge-porn-and-search.html. Google's "Removal Policy" is available at https://support.google.com/websearch/answer/2744324.

CHAPTER 7: INTELLECTUAL PROPERTY

Page 605, after conclusion of "Copyright Overview":

An *en banc* decision from the Ninth Circuit rejected an actor's request for a preliminary injunction enjoining the dissemination of an anti-Islamic film in which she appeared for just over five seconds. See *Garcia v. Google*, 786 F.3d 733 (9th Cir. 2015) (en banc). Plaintiff Cindy Lee Garcia claimed that she did not know her performance would be dubbed over and inserted into a controversial film called *Innocence of Muslims*, which some credited with causing violence in the Middle East. Garcia asserted that as a result of its distribution, she had received multiple death threats. Although she asserted multiple claims in her complaint against Google and the film's director, including ones for defamation and intentional infliction of emotion distress (and may have also been able to assert claims for breach of contract and violations of her right of publicity), her petition for injunctive relief was based solely on her claim that she held the copyright in her performance.

The court reversed a panel decision enjoining Google from hosting on YouTube or any other Google-controlled website the portion of the film containing the plaintiff's performance. The court concluded that Garcia did not have a recognizable copyright in her performance within a larger film, adding that "[t]reating every acting performance as an independent work would not only be a logistical and financial nightmare, it would turn cast of thousands [in movies like *Ben-Hur* or *Lord of the Rings*] into a new mantra: copyright of thousands." The court also held that Garcia failed to demonstrate irreparable harm. Not only did she wait several months before seeking injunctive relief, the court explained, but also the harms she claimed – severe emotional distress and reputational harm – are not the sort of harms copyright law protects.

Page 631, at conclusion of "Trademark Overview":

In July 2015, a federal district court judge rejected a First Amendment challenge to the U.S. Patent & Trademark Office's decision to cancel the Washington Redskins trademarks because they are offensive to Native Americans. *Pro-Football, Inc. v. Blackhorse*, 112 F. Supp. 3d 439 (E.D. Va. 2015). In cancelling the trademarks, the agency relied on a law prohibiting the recognition of a mark that "consists of or comprises immoral, deceptive, or scandalous matter; or matter which *may disparage* or falsely suggest a connection with persons, living or dead, institutions, beliefs, or national symbols, or bring them into contempt, or disrepute . . . ." 15 U.S.C. § 1052(a) (emphasis added). The district court held that the agency's decision did not violate the First Amendment because the decision to recognize a trademark is government speech, not private speech. The court relied heavily on a recent Supreme Court decision holding that specialty license plates are government speech not subject to the free speech limitations of the First Amendment. See *Walker v Texas Div., Sons of Confederate Veterans, Inc*., 135 S. Ct. 2239 (2015) (rejecting First Amendment challenge to Texas's refusal to issue a specialty license plate containing a confederate flag).

CHAPTER 8: CIVIL AND CRIMINAL LIABILITY

Page 684, after *ACLU v. Alvarez*:

Courts have increasingly recognized a right to record police officers, but no consensus has emerged. Both the Eleventh and First Circuits have recognized a First Amendment right, subject to reasonable time, manner, and place restrictions, to photograph or videotape police conduct. Smith v. City of Cumming, 212 F.3d 1332, 1333 (11th Cir. 2000); Gilk v. Cunniffe, 655 F.3d 78 (1st Cir. 2011). Two district courts in the Third Circuit, however, have been much more reluctant to embrace a broad First Amendment right to record the police. One judge in the Eastern District of Pennsylvania held that "the right to record matters of public concern is not absolute," Fleck v. Trustees of Univ. of Pennsylvania, 995 F. Supp. 2d 390, 407 (E.D. Pa. 2014), while another judge determined the right to videotape police officers extends only to "expressive" conduct or conduct "otherwise critical of the government." Fields v. City of Philadelphia, No. CV 14-4424, 2016 WL 2754014, at *4 (E.D. Pa. Feb. 19, 2016).

The Department of Justice has weighed in on this issue. In connection with a case in which the Baltimore Police Department confiscated a person's phone after he recorded police officers forcibly arresting his friend, the Department of Justice wrote in a Statement of Interest, "The right to record police officers while performing duties in a public place . . . [is] consistent with our fundamental notions of liberty, promote the accountability of our governmental officers, and instill public confidence in the police officers who serve us daily." *Christopher Sharp, Plaintiff, v. BALTIMORE CITY POLICE DEPARTMENT, et al., Defendants*, 2012 WL 9512053 (D. Md.).

The Court of Appeals for the Seventh Circuit has issued a potentially important opinion offering a much more limited view of the First Amendment's application to laws that punish the gathering and dissemination of information of public concern. In *Dahlstrom v. Sun-Times Media LLC*, 777 F.3d 937 (7th Cir. 2015), the Seventh Circuit held that the First Amendment did not protect a newspaper sued for obtaining and publishing "personal information" about police officers contained in motor vehicle records. In reaching this decision, Seventh Circuit distinguished both *Bartnicki v. Vopper* and its own prior decision in *ACLU of Illinois v. Alvarez*, 679 F.3d 583 (7th Cir. 2012), which is already included in this chapter.

DAHLSTROM V. SUN-TIMES MEDIA, LLC
777 F.3d 937 (7th Cir. 2015)

The Driver's Privacy Protection Act ("DPPA") prohibits individuals from knowingly obtaining or disclosing "personal information" from a motor vehicle record. In this interlocutory appeal, five Chicago police officers brought suit against Sun–Times Media, alleging that the publishing company violated the DPPA by obtaining each officer's birth date, height, weight, hair color, and eye color from the Illinois Secretary of State's motor vehicle records, and publishing that information in a newspaper article that criticized a homicide investigation lineup in which the officers participated. Sun–Times moved to

dismiss the officers' complaint, arguing that the published information does not constitute "personal information" within the meaning of the DPPA, or, in the alternative, that the statute's prohibition on acquiring and disclosing personal information from driving records violates the First Amendment's guarantees of free speech and freedom of the press.

As to the question of statutory interpretation, we conclude that the DPPA's definition of "personal information" extends to the details Sun–Times published here. With respect to the First Amendment challenge, we conclude that Sun–Times possesses no constitutional right either to obtain the officers' personal information from government records or to subsequently publish that unlawfully obtained information. We therefore affirm the district court's denial of Sun–Times's motion to dismiss.

Twenty-one-year-old David Koschman died after an April 25, 2004 altercation with R.J. Vanecko, a nephew of Richard M. Daley, then-Mayor of Chicago. Given Vanecko's political connections, the subsequent Chicago Police Department investigation was highly publicized. Several weeks after the incident, the Department placed Vanecko in an eyewitness lineup, in which five Chicago police officers participated as "fillers." These officers—[the] plaintiffs—closely resembled Vanecko in age, height, build, and complexion. When eyewitnesses failed to positively identify Vanecko as the perpetrator, the Department declined to charge him. The Department closed the Koschman investigation in March 2011.

Suspicious that the Department may have manipulated the homicide investigation because of Vanecko's high-profile Chicago connections, defendant Sun–Times Media published a series of investigative reports criticizing the Department's handling of the case. One such report, a November 21, 2011 article featured in the *Chicago Sun–Times* (and on the news-paper's website), questioned the legitimacy of the Vanecko lineup. The article, "Daley Nephew Biggest Guy on Scene, But Not in Lineup," highlights the physical resemblance between Vanecko and the lineup "fillers" in an effort to demonstrate that the Officers resembled Vanecko too closely for the lineup to be reliable. To support this accusation, Sun–Times published photographs of the lineup, as well as the names of each of the five officer "fillers." Sun–Times obtained these names and photographs from the Chicago Police Department pursuant to a request under the Illinois Freedom of Information Act ("FOIA"). However, the *Sun–Times* article featured not only the lineup photographs and the Officers' full names, but also the months and years of their birth, their heights, weights, hair colors, and eye colors. Sun–Times credited the Chicago Police Department and the Illinois Secretary of State as sources. The Officers contend—and Sun–Times has not disputed—that Sun–Times knowingly obtained this additional identifying information from motor vehicle records maintained by the Secretary of State.

The DPPA states that, subject to certain limited exceptions not relevant here, "[i]t shall be unlawful for any person knowingly to obtain or disclose personal information[ ] from a motor vehicle record." A separate provision of the Act specifically proscribes officers, employees, and contractors of state departments of motor vehicles from

knowingly disclosing that same information.

The Officers sued Sun–Times claiming that by acquiring and publishing each Officer's approximate birth date, height, weight, hair color, and eye color, Sun–Times violated their rights under [the DPPA]. Sun–Times moved to dismiss the Officers' complaint for failure to state a claim upon which relief can be granted, pursuant to Fed. Rule. Civ. P. 12(b)(6). Sun–Times contends that the published information does not fall within the DPPA's definition of "personal information," or, alternatively, that if the DPPA bars Sun–Times from publishing this truthful information of public concern, the statute violates the First Amendment's guarantees of freedom of speech and freedom of the press. Sun–Times also argues that the Officers' requested injunction, if issued, would amount to an unconstitutional prior restraint on speech.

[The district court denied the Sun-Times's motion.] We granted Sun–Times's petition for interlocutory appeal.

[The Seventh Circuit first concluded that the details the Sun-Times obtained from the officers' driving records constitute "personal information" under the DPPA. The court then addressed Sun-Times's First Amendment defenses.]

Sun–Times first argues that the DPPA's prohibition on obtaining personal information from motor vehicle records interferes with the ability of the press to gather the news. Sun–Times argues that, although on its face the DPPA is aimed at limiting *access* to motor vehicle records at the outset, the statute was nevertheless enacted to suppress speech—albeit at an earlier point in the speech process. The DPPA, according to Sun–Times, restricts speech because it restricts the news media's ability to gather and report the news. Sun–Times looks primarily to our opinion in *ACLU of Illinois v. Alvarez* to support its contention. Sun–Times contends that our reasoning in *ACLU* indicates that although the DPPA does not prevent Sun–Times from publishing personal information obtained through lawful means, the Act's ban on the acquisition of personal information from an individual's motor vehicle record amounts to an unconstitutional burden on speech.

However, *ACLU* is distinguishable on several grounds. While the Illinois eavesdropping statute's effect on First Amendment interests was "far from incidental" because it banned "*all* audio recording of *any* oral communication," the same is not true of the DPPA's prohibition on the acquisition of personal information from a single, isolated source. It can hardly be said that this targeted restriction renders Sun–Times's right to publish the truthful information at issue here—much of which can be gathered from physical observation of the Officers or from other lawful sources (including, of course, a state FOIA request)—"largely ineffective." Further, in forbidding only the act of peering into an individual's personal government records, the DPPA protects privacy concerns not present in *ACLU*. If a member of the press observed one of the Officers in public—for example, during a traffic stop—he could publish any information gleaned from that interaction without offending the DPPA. By contrast, the Illinois eavesdropping statute operated as a total ban on recording police officers' activities, even when they

were "performing their duties in public places and speaking at a volume audible to bystanders."

The nature of the restricted form of expression also figured prominently in our *ACLU* analysis. We noted that "[a]udio and audiovisual recording are media of expression commonly used for the preservation and dissemination of information and ideas and thus are included within the free speech and free press guaranty of the First and Fourteenth Amendments." We also identified photography, note-taking, and the posting of signs as other common media of expression. Yet while the eavesdropping statute "restrict [ed] the use of a *common, indeed ubiquitous, instrument of communication,*" the act of harvesting information from driving records is hardly such an instrument. We are therefore unpersuaded by Sun–Times's attempt to analogize a total ban on recording police officers' actions in public to the DPPA's effort to maintain the privacy of personal information contained in an individual's driving record.

For the foregoing reasons, we conclude that the DPPA's prohibition on knowingly obtaining an individual's personal information from motor vehicle records does not trigger heightened First Amendment scrutiny and instead requires only rational basis review. Because limiting public access to driving records is rationally related to the government's legitimate interest in preventing "stalkers and criminals [from] acquir[ing] personal information from state DMVs," the restriction easily satisfies the deferential rational basis standard.

Although we have established that the DPPA's limitation on obtaining personal information is not a restriction on speech at all, the Act's prohibition on *disclosing* that information is a direct regulation of speech. [The court then concludes that "DPPA is content neutral because its public safety goals are "unrelated to the content of [the regulated] expression."]

The Supreme Court has established that "if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order." Sun–Times, however, cites no authority for the proposition that an entity that acquires information by breaking the law enjoys a First Amendment right to disseminate that information. Instead, all of the many cases on which Sun–Times relies involve scenarios where the press's initial acquisition of sensitive information was lawful.

Sun–Times's acquisition of the Officers' personal information invaded their established rights under the DPPA. Although Sun–Times claims that, in acquiring and disclosing truthful information, it engaged only in "perfectly routine, traditional journalism," it cannot escape the fact that it acquired that truthful information *unlawfully*.

Given this distinction, we enter uncharted territory in our analysis of what the Supreme Court has identified as a "still-open question"—that is, "whether, in cases where information has been acquired *unlawfully* by a newspaper[,] ... government may ever

punish not only the unlawful acquisition, but the ensuing publication as well." *Bartnicki*.

The DPPA's prohibition on disclosing individuals' personally identifiable information—separate and apart from its ban on obtaining that information—advances two government interests, both of which relate to the Act's underlying public safety goals: first, the interest in removing an incentive for parties to unlawfully obtain personal information in the first instance; and second, the interest in minimizing the harm to individuals whose personal information has been illegally obtained. Analyzing similar asserted interests with respect to a federal ban on the disclosure of illegally intercepted cellular telephone conversations, the *Bartnicki* Court "assume[d] that those interests adequately justify the [statute's] prohibition ... against the interceptor's own use of information that he or she acquired by violating [the statute]."

In evaluating the proffered interest in deterrence, however, the *Bartnicki* Court was unwilling to accept the government's contention that a ban on disclosure by individuals who lawfully came into possession of intercepted communications would meaningfully discourage the initial unlawful interception by a third party. Here, there is no intervening illegal actor: Sun–Times itself unlawfully sought and acquired the Officers' personal information from the Secretary of State, and proceeded to publish it. Where the acquirer and publisher are one and the same, a prohibition on the publication of sensitive information operates as an effective deterrent against the initial unlawful acquisition of that same information. Such acquisition carries little benefit independent of the right to disseminate that information to a broader audience. We therefore conclude that the government's deterrence interest is both important and likely to be advanced by the DPPA's ban on Sun–Times's disclosure of the Officers' personal information.

The Supreme Court has also recognized the importance of the government's second asserted interest—protecting the privacy of individuals whose personal information has been illegally obtained. [W]hile the *Bartnicki* Court recognized the substantial state interest in privacy protection, it nevertheless determined that, under the applicable facts, "privacy concerns give way when balanced against the interest in publishing matters of public importance."

We conclude, however, that the balance in the instant case tips in the opposite direction. Although the *Sun–Times* article relates to a matter of public significance—the allegation that the Chicago Police Department manipulated a homicide investigation—the specific details at issue are largely cumulative of lawfully obtained information published in that very same article, and are therefore of less pressing public concern than the threats of physical violence in *Bartnicki.* While Sun–Times provided details of the Officers' physical traits to highlight the resemblance between the "fillers" and Vanecko, most of the article's editorial force was achieved through publication of the lineup photographs that Sun–Times obtained through its FOIA request—the value added by the inclusion of the Officers' personal information was negligible. Each Officer's height is evident from the lineup photographs, while their weights and ages are relevant only to the extent that they increase the Officers' resemblance to Vanecko—a resemblance that the photographs independently convey. And, although identifying the Officers' hair and eye colors may

add some detail to the published black-and-white photographs, their personal information is largely redundant of what the public could easily observe from the photographs themselves. Therefore, Sun–Times's publication of the Officers' personal details both intruded on their privacy and threatened their safety, while doing little to advance Sun–Times's reporting on a story of public concern. Certainly, in context, the significance of the Officers' personal information does not rise to the level of the threats of physical violence at issue in *Bartnicki,* and therefore does not override the government's substantial interest in privacy protection. In sum, we conclude with respect to the first prong of the intermediate scrutiny analysis, that the government's asserted interests are both important and furthered by the DPPA's prohibition on disclosure.

As for the second prong of the analysis, both of the government's interests—(1) deterring the initial illegal acquisition of personal information, and (2) protecting the privacy of individuals whose information has been illegally obtained—are unrelated to the suppression of free expression and instead relate to the promotion of public safety. Finally, we inquire whether the DPPA is narrowly tailored such that it encroaches upon First Amendment freedoms only to the extent necessary to further those government interests. The DPPA's disclosure prohibition contains several safeguards characteristic of narrow tailoring: it is content neutral, it permits publication of the same information gathered from lawful sources, it imposes no special burden upon the media, and it has a scienter requirement ("knowingly") to provide fair warning to potential offenders. The prohibition also contains fourteen "permissible use" exceptions, which permit disclosure under those circumstances deemed unlikely to threaten an individual's personal safety. Given these features, we conclude that the law does not burden substantially more speech than necessary to further the government's legitimate interests, and therefore withstands intermediate scrutiny.

For these reasons, we conclude that the DPPA's prohibition on disclosing the Officers' personal information does not violate Sun–Times's First Amendment rights. As this is an as-applied challenge, our holding is limited to the facts and circumstances of this case. We do not opine as to whether, given a scenario involving lesser privacy concerns or information of greater public significance, the delicate balance might tip in favor of disclosure. We hold only that, where members of the press unlawfully obtain sensitive information that, in context, is of marginal public value, the First Amendment does not guarantee them the right to publish that information. The district court therefore did not err in denying Sun–Times's motion to dismiss the Officers' claim that Sun–Times violated their rights under the DPPA.

Page 716, after Note 6:

7. A much less commonly invoked section of the Espionage Act, § 793(f), gained attention in 2016 after Hillary Clinton's email controversy. During her time as Secretary of State, Ms. Clinton maintained a private email server, separate from the secured State Department server, through which she discussed some confidential topics and materials with her aides over email. In July 2016, the Department of Justice decided not to press criminal charges under § 793(f) after FBI Director James Comey concluded that "no

reasonable prosecutor would bring such a case." Mark Landler and Eric Lichtblau, *Stern Rebuke, but No Charges, for Clinton*, N.Y. TIMES, July 6, 2016, at A1. Section 793(f) provides as follows:

> Whoever, being entrusted with or having lawful possession or control of [any of the items mentioned in § 793(d)], (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of its trust, or lost, or stolen, abstracted, or destroyed ... fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer . . . .

18 U.S.C. § 793(f) (2014). Although some have argued that using a private server to transmit classified information was "grossly negligent," it is hardly clear that the remaining language of this almost 100-year-old statute covers Clinton's actions. As Professor Steve Vladeck wrote, "The better way forward is for Congress to do something it's refused to do for more than 60 years: carefully and comprehensively modernize the Espionage Act, and clarify exactly when it is, and is not, a crime to mishandle classified national security secrets." Steve Vladeck, *Hillary Clinton and the Espionage Act*, SLATE.COM (July 6, 2016), http://www.slate.com/articles/news_and_politics/jurisprudence/2016/07/the_hillary_clinton_email_scandal_shows_the_espionage_act_is_outdated.html.

Page 727, after Note 2:

3. In response to technological advancements that led to smaller and more discrete recording equipment and the backlash received by undercover videos, the agricultural sector has pushed for laws criminalizing secret recordings on farms without the owner's consent. These anti-whistleblower laws have been called "ag-gag laws" and have raised significant First Amendment concerns, specifically because they seem targeted towards prohibiting specific types of viewpoints. Seven states have ag-gag laws, although a federal district court in Idaho recently held that state's law was unconstitutional. Animal Legal Def. Fund v. Otter, 118 F. Supp. 3d 1195, 1199 (D. Idaho 2015). An appeal is pending before the Ninth Circuit. For more in-depth analysis of the constitutionality of these "ag-gag" laws as well as other government attempts to regulate video recordings, see Justin Marceau & Alan Chen, *Free Speech and Democracy in the Digital Age*, 116 COLUM. L. REV. 991 (2016).

Page 759, after Note 5:

6. Plaintiffs may use other causes of action to seek recovery from newsgathering practices. In *Chanko v. Am. Broad. Companies Inc*., 27 N.Y.3d 46 (2016), the highest court in New York held that the relatives of a deceased hospital patient filmed while receiving treatment in an emergency room stated a claim for breach of confidentiality against the hospital and chief surgical resident. The hospital and resident had allegedly given permission to ABC to film in ER for a documentary called *N.Y. Med* without

receiving consent from the patient for the filming or the presence of the camera crew. The court made clear that breach of confidentiality claims do not require the disclosed information to be embarrassing or the sort of information a patient would want to keep secret. In addition, the court held that obscuring the identity of patient in the broadcast did not impact the plaintiffs' breach of confidentiality claims because "the complaint expressly alleges an improper disclosure of medical information to the ABC employees who filmed and edited the recording, in addition to the broadcast itself."

The family members did not appeal the dismissal of their breach of confidentiality claim against ABC, and the court held that claims that ABC aided and abetted the breach of confidentiality were not properly before it. The court also upheld the dismissal of the claim for intentional infliction of emotional distress against ABC. The court held that although recording someone's last moments of life was "offensive" and "would likely be considered reprehensible by most people," it did not rise to the level of "extreme and outrageous conduct" necessary to state a claim. The court's distinction between "offensive" conduct and "extreme and outrageous conduct" illustrates one important difference between intrusion claims, as we saw in *Shulman*, and intentional infliction of emotional distress claims.

7. In *Haldimann and Others v. Switzerland* 21830/09 Judgment 24.2.2015, the European Court of Justice held that the criminal convictions of four journalists for recording and broadcasting an interview using hidden cameras violated Article 10 of the European Convention on Human Rights.

Journalists for the Swiss German television station SF DRS used hidden cameras to capture an interview between one of the journalists posing as a customer and an insurance broker. This interview was conducted as part of an investigation into broader public debate regarding the business practices of insurance brokers generally. The journalists used portions of the taped interview in a subsequent broadcast, although the broker's face and voice were disguised. A Swiss court held that the journalists were guilty of violating the criminal law against recording and broadcasting conversations without permission and levied fines. Relying on its prior decision in *Axel Springer* [see pages 547-54], the ECHR weighed the freedom of expression against the right to a private life and concluded that the report contributed to an important public debate regarding the specific practices of insurance brokers and the lack of consumer protections and that the veracity of the report was not in dispute. In addition, the report did not focus specifically on the broker filmed but rather on the insurance broker industry more generally. As a result, the ECHR concluded, the interference with the private life of the broker did not outweigh the contribution of the recording and broadcast to the public debate.

7. Unmanned aircraft systems (UAS), also commonly called "drones," are increasingly used as a newsgathering tool. (They can also be used for many other purposes, including, for example, inspecting crops, pipes, power lines, bridges, houses, parks, and antennae; aiding certain rescue operations; and evaluating wildlife nesting areas.)

After receiving extensive public comment on its proposed regulations regulating the use of non-hobbyist small UAS, the FAA announced new rules governing small (under 55 pounds) UASs in June 2016. In addition to rules restricting who can operate a drone, these new rules provide that drones must be in the line of sight of the operator at all times, cannot fly over people, cannot be more than 400 feet high over the ground or from a structure, and cannot operate at night. The FAA has stated that it will consider waiver requests and will soon launch new rule making proceedings to explore rules for using drones over people. The new regulations, which total over 600 pages, can be found at http://www.faa.gov/uas/media/RIN_2120-AJ60_Clean_Signed.pdf. The FAA rules expressly state that they do not preempt state and local drone laws. As a result, anyone using a drone must also consult the laws of the applicable jurisdiction.

With these new rules paving the way for commercial use of drones, journalistic use of drones will likely increase dramatically. See http://www.poynter.org/2016/why-2016-could-be-a-breakout-year-for-drone-journalism/390386/ At the same time, drones equipped with cameras or sensors raise obvious privacy concerns. Current privacy torts, like intrusion and publication of private fact, arguably provide minimal protection against drone surveillance in public places. In its recent rulemaking, the FAA recognized the significance of privacy concerns as well as the lack of consensus on how to address them. Regarding its primary mission to protect safety, not privacy, the FAA nevertheless strongly urged state and local governments to adopt privacy rules and encouraged drone users to follow the recommended privacy guidelines generated by the National Telecommunications and Information Administration (NTIA). These guidelines recommend the implementation of policies regarding the gathering and retention of personal information. In addition, the guidelines contain a list of common-sense suggestions for "Neighborly Drone Use," such as: "If anyone raises privacy, security, or safety concerns with you, try and listen to what they have to say, as long as they're polite and reasonable about it." These voluntary best practices can be found here. https://www.ntia.doc.gov/files/ntia/publications/voluntary_best_practices_for_uas_privacy_transparency_and_accountability_0.pdf.

These new FAA regulations do not apply to anyone who operates a small UAS "strictly for hobby or recreational use." In May 2016, the FAA issued a guidance memorandum clarifying that student use of drones "in furtherance of receiving instruction at accredited educational institutions" – such as students in journalism programs -- constitutes use of an aircraft for hobby or recreational purposes because such students are not using drones for "compensation" or for business purposes. http://www.faa.gov/uas/resources/uas_regulations_policy/media/interpretation-educational-use-ofuas.pdf.

Media attorneys Nabiha Syed and Michael Berry have written a useful summary of some of the fascinating practical and legal questions regarding the media's use of drones. *See* Nabiha Syed & Michael Berry, *Journo-Drones: A Flight Over the Legal Landscape*, 30-JUN COMM. LAW. 1 (June 2014).

The Court of Justice of the European Union has held that surveillance cameras installed outside a home that capture images of people on public property are subject to the EU's data privacy protection laws. Case C-212/13, František Ryneš v Úřad pro ochranu osobních údajů, http://curia.europa.eu/juris/liste.jsf?num=C-212/13#. In this case, Frantisek Rysens installed a camera over the front entrance of his home after unknown individuals had attacked it. When his window was broken, Rysens gave the police footage from his camera depicting two suspects. The CJEU held that the homeowner violated the EU law by failing to obtain the consent of individuals of these suspects prior to filming. The Court concluded Rysens was not entitled to the exception in EU for filming done "in the course of purely personal or household activity" because his camera captured images beyond his property and in a public space. This decision has significant ramifications for filming people without their consent with a drone.

CHAPTER 9: INDIRECT RESTRAINTS

Page 844, Note 4:

Replace citation to Eastern District of Michigan decision with a citation to a recent Sixth Circuit decision affirming it: *Convertino v. DOJ*, 795 F.3d 587 (6th Cir. 2015), and add the following summary of the Sixth Circuit's decision.

In this case, *Detroit Free Press* reporter David Ashenfelter was subpoenaed to identity his source for leaked documents and information regarding the Department of Justice's investigation into potential professional misconduct by former U.S. assistant attorney Richard Convertino in connection with a terrorism prosecution of three Detroit-area men. Conventino brought a Privacy Act case against the government based on these alleged leaks. At his deposition, Ashenfelter asserted his Fifth Amendment right against self-incrimination in response to some of Convertino's questions. The district court rejected Convertino's motion to compel, holding that Ashenfelter had a reasonable basis for fearing that answering the questions would entail self-incrimination. The Sixth Circuit affirmed.

In reaching its decision, the Sixth Circuit rejected the argument that Ashenfelter could not invoke the Fifth Amendment because it was not likely that the government would prosecute the reporter for the unauthorized receipt, retention, or disclosure of confidential information and documents. The court made clear "it is not the likelihood but rather the possibility of prosecution that matters in the assertion of privilege." The court concluded that "Convertino's arguments about the lack of apparent political will to prosecute Ashenfelter, or about the unsettled points of law that might ultimately render a criminal prosecution unsuccessful, are therefore without merit. A witness is not required to shoulder such risks."

In addition, the court said it was irrelevant that Attorney General Eric Holder had made a statement in January 2015 in the context of the James Risen subpoena that DOJ would not prosecute a reporter "for doing his job." [The *Risen* case is discussed below.] The court noted that "[t]he former Attorney General's statement did not constitute a grant of immunity to journalists, and his assurances might not outlast his own, now completed, tenure. Even if Holder's statement reflected a policy internally enforced by the DOJ, Ashenfelter could not invoke that policy to bar a criminal prosecution."

Page 874, after Note 9:

The Supreme Court denied reporter James Risen's petition for a writ of certiorari in June 2014. Nevertheless, Risen continued to insist that he would rather go to jail than reveal his sources. Shortly before Jeffrey Sterling's trial in January 2015, Attorney General Eric Holder reversed course and announced that prosecutors would not press Risen to reveal any confidential sources because under as long as Holder was AG, the federal government "will not prosecute any reporter for doing his or her job." A jury ultimately convicted Jeffrey Sterling on nine felony counts relating to the unauthorized

disclosure of national security information, leading critics to call into question prosecutors' claims that Risen's testimony was essential and to renew their arguments for the passage of a robust federal shield law. *See* Matt Apuzzo, *C.I.A. Officer is Found Guilty in Leak Tied to Times Reporter*, N.Y. TIMES (Jan. 26, 2015), at A1.

Page 901, at end of Note 3:

In *American Civil Liberties v. Clapper*, 785 F.3d 787 (2d Cir. 2015), the Second Circuit held that the ACLU and other civil liberties groups had standing to challenge the government's surveillance program and held that the program was illegal because it was not statutorily authorized. In this case, the government did not dispute that it had collected the metadata associated with the plaintiffs' telephone calls; instead, the government argued that the plaintiffs lacked standing because they could not demonstrate that the government had reviewed this metadata. The Second Circuit concluded the mere collection of this information constituted a "seizure" under the Fourth Amendment, and that in any event the government conceded that the plaintiffs' metadata was included in the database that is searched electronically. The court also held that the plaintiffs had standing to allege a First Amendment violation that the surveillance chilled the associational rights of themselves and their clients and donors.

Although the court concluded that the metadata collection program was illegal, it declined to enter a preliminary injunction enjoining it because Section 215 was due to expire in a few weeks and was the subject of intense congressional debate. Noting the government's claims that the program was essential to national security, the panel held that "[a]llowing the program to remain in place for a few weeks while Congress decides whether and under what conditions it should continue is a lesser intrusion on appellants' privacy than they faced at the time this litigation began." In June, Congress passed new legislation that gives the government six months to end its bulk collection of private telephone records. Private telecommunications companies are now required to retain phone call metadata, and the government can obtain this information on a case-by-case basis with a court order.

Page 921, at end of Note 6:

Some subpoenas seeking to unmask the identities of anonymous parties have failed for lack of personal jurisdiction. In *AF Holdings LLC v. Does 1-1058*, 752 F.3d 990 (D.C. Cir. 2014), for example, the court rejected subpoenas served on internet service providers seeking to gain information about 1,058 IP addresses from which individuals illegally downloaded a copyrighted pornographic film using BitTorrent. The court held that in cases involving subpoenas to anonymous parties, a plaintiff must demonstrate a good-faith belief that discovery would reveal that the court had personal jurisdiction over the target. Here, the court explained, the plaintiff had made no attempt to limit the scope of its subpoenas to internet service providers to seek the identify of subscribers who are residents in the District of Columbia or at least downloaded the film there, the only two conceivable bases for personal jurisdiction. The court noted that very inexpensive geolocation technology would have enabled them to tailor their subpoenas appropriately.

CHAPTER 10: ACCESS TO INFORMATION

Page 994, after *North Jersey Media Group, Inc. v. Ashcroft*:

The differences between the Third and Sixth Circuit opinions on removal proceedings illustrate the difficulties of applying the "history and logic" test outside the context of judicial proceedings. A rigid history requirement is often fatal to right of access claims, and the logic prong gives courts little meaningful guidance.

For example, the Supreme Court of Georgia recently rejected a death-row prisoner's argument that the state's execution-participant confidentiality statute violates the First Amendment. *See* Owens v. Hill, 758 S.E.2d 794 (Ga. 2014). Warren Lee Hill sought the names and other identifying information for all persons and entities that would be involved in his execution, including those who manufacture the drug or drugs to be used. The court first explained that although there has been some history of permitting the public to view executions, the identity of the executioner has traditionally been concealed in order to avoid harassment or retaliation. The court then reasoned that "on balance" concealing the identity of all involved parties, including the drug manufacturers, made Georgia's execution process "more timely and orderly" by avoiding the risk that persons and entities essential to the execution would be unwilling to participate. Noting the recent problems with botched executions in other states, the dissent would have ruled for Hill on due process grounds, arguing that the secrecy around executions creates "very secret star chamber-like proceedings," and that concerns that openness would hinder the execution process are out of place "when the state is carrying out the ultimate punishment."

Page 1019, in last paragraph:

In April 2015, the Department of Justice revised the FOIA regulations to make clear that the definition of "a representative of the news media" exempt from the payment of search fees includes news organizations that operate solely on the Internet.

Page 1026, after Note 2:

3. Courts often accept government's claims that government records are exempt under Exemption 1 of FOIA, which permits the government to withhold records that are "specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy" and that "are in fact properly classified pursuant to such Executive order." 5 U.S.C. § 552(b)(1). *See*, *e.g.*, ACLU v. U.S. Dep't of Justice, 640 Fed. App. 9 (Mem.) (per curiam) (relying on Exemption 1 to reject FOIA request for CIA records relating the use of armed drones to conduct "targeted killings"). Center for Constitutional Rights v. Central Intelligence Agency, 765 F.3d 161 (2d Cir. 2014) (affirming denial of FOIA request to the CIA, Department of Defense, and DOJ for images and photographs of detainees held at Guantanamo Bay).

But at times FOIA plaintiffs have been able to defeat Exemption 1 claims. In a particularly significant case, the Second Circuit held that the Department of Justice's Office of Legal Counsel (OLC) was required to release documents containing a legal analysis of the government's use of drones for the targeted killing of U.S. citizens. *See* N.Y. Times Co. v. U.S. Dep't of Justice, 756 F.3d 100 (2d Cir. 2014). The court rejected the government's reliance on FOIA's Exemption 1 (national security) and Exemption 5 (deliberative process privilege) on the ground that the government had waived the confidentiality of this information by disclosing the same information itself as part of an apparent "public relations campaign" to convince people of the merits of the program. The court cited a number of statements made by public officials as well as the official release of a DOJ "white paper" explaining the government's legal analysis supporting the program in same detail as the desired OLC memorandum.

4. The increase in the use of police body cameras around the country has led to some questions about who has the right to see the footage. Although the cameras can promote transparency and accountability, many states and cities arguing for limits on the public's access cite the privacy concerns of individuals captured in the footage as well as the integrity of criminal investigations that rely on the footage. The current and proposed restrictions on public access vary widely, but in some instances, legislatures have passed or are considering proposals that would exempt body camera footage from state FOIA laws. For a helpful map summarizing state legislation and police department regulations regarding pubic access to police body cameras, https://www.rcfp.org/bodycams.

CHAPTER 11: GOVERNMENT REGULATION OF ELECTRONIC MEDIA

Page 1121, at the end of Note 4:

In response to the D.C. Circuit's December 2014 opinion, the FCC began rulemaking proceedings and ultimately issued a new Open Internet Order, 80 Fed. Reg. 19,738, *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0312/FCC-15-24A1.pdf. Significantly, this lengthy Order declares that the FCC's authority for its Open Internet rules rests on Title II of the Communications Act and Section 706 of the Telecommunications Act of 1996. The FCC reclassified broadband Internet access providers as telecommunications services under Title II but announced that the agency would refrain (or "forebear") from enforcing provisions of Title II that it deemed not relevant to modern broadband service, such as rate regulation. Classifying broadband providers as telecommunications services allowed the FCC to impose anti-blocking (providers may not block lawful content), anti-throttling (providers may not decrease connection speeds to lawful content) and anti paid-prioritization (providers may not prioritize connection speeds in favor of one website in exchange for consideration) regulations on those providers. The FCC prepared a short "fact sheet" about the 2015 Order; it is available at https://apps.fcc.gov/edocs_public/attachmatch/DOC-331869A1.pdf.

On June 14, 2016, the D.C. Circuit ruled that the FCC had the authority to enact the Open Internet Order. United States Telecom Ass'n v. Fed. Commc'ns Comm'n, No. 15-1063, 2016 WL 3251234 (D.C. Cir. June 14, 2016). Basing its new rule on the reasoning in *National Cable & Telecommunications Ass'n v. Brand X Internet Services*, 545 U.S. 967 (2005), the FCC looked to the end-users' perception of what kind of service that broadband providers render to determine whether broadband is a telecommunications network, and therefore subject to more regulations, or an information service. Broadband providers in the early 2000s, like AOL, included email and other applications in their service, and end-users looked to AOL to provide both their Internet connection as well as those other information services. However, by 2016, if broadband providers even still offer such additional services, they are usually viewed as ancillary or in addition to providing an Internet connection. The D.C. Circuit concluded that because broadband providers are now reasonably viewed as providing a telecommunication service and are classified as such, they may be regulated to enforce the FCC's vision of an open Internet.