Communications Lawyer
Publication of the Forum on Communications Law
American Bar Association
Volume 33, Number 1 Summer 2017
THE JOURNAL OF MEDIA, INFORMATION, AND COMMUNICATIONS LAW

In this issue

The Myth of Police Officer Privacy

STEVE ZANSBERG AND DANA GREEN

> "Upon careful review, we have determined that disclosure of the files you have requested -- the police department's internal affairs investigation into former officer Smith's conduct (which resulted in his placement on administrative leave, prior to his resignation) -- would constitute an unwarranted invasion of officer Smith's privacy. Accordingly, we hereby deny your request to inspect those records."

The statement above is not the denial of an actual request to inspect a police internal affairs file. Nevertheless, it will be familiar to many of you as the type of denial that police departments, across the land, issue with regularity.[1] "Officer privacy" has also been cited as a potential basis for withholding footage shot on police body-worn cameras.[2] This purported "officer's right to privacy" has even been invoked as the basis for preventing ordinary citizens and journalists from photographing or videotaping an officer in discharging his or her official duties.[3]

While some states have explicit statutory provisions mandating the public availability of completed police internal investigation files,[4] several states either categorically close all such records to the public,[5] or they allow records custodians varying degrees of discretion.[6] And, as the hypothetical denial above demonstrates, police chiefs and sheriffs regularly (though not uniformly) cite officers' "right to privacy" as their reason for withholding police internal investigation files, even when those records reflect the officer's official conduct performed on a public street, sidewalk, or park.

So, is there *any* legitimacy to this claim? Unfortunately, the argument has had some traction, with some courts giving deference to police departments' (and police unions') assertions of "officer privacy." This article argues that those "outlier" decisions are erroneous as a matter of law. This article examines the claim of "officer privacy" as it has been raised in a variety of related contexts: state and federal open records laws, officers' claims of civil rights violations following the unconsented-to governmental release of such information, and common-law invasion of privacy claims. Although these are distinct areas of law, each with its own doctrinal foundations, we believe that a fair and objective review of the case law leads to one inescapable conclusion: law enforcement officers do NOT have a *reasonable* expectation of privacy with respect to records memorializing or discussing their official conduct, while on duty. Thus, it is time to lay "the myth of police officer privacy" to rest, once and for all.

STATE AND FEDERAL FOI LAWS

State and federal freedom of information ("FOI") laws routinely contain exemptions from the right of public access for records where disclosure would constitute an "unwarranted invasion of personal privacy" (or words to that effect).[7] Often, these are general exemptions, not restricted to police or public employee records, that apply to any records containing "personal"

(Continued on page 5)

Steve Zansberg *is a partner at Levine Sullivan Koch & Schulz LLP in Denver, Colorado and past Chair of the ABA Forum on Communications Law.* **Dana Green** *is an associate at Levine Sullivan Koch & Schulz LLP in Washington, D.C.*

FROM THE CHAIR

What Really Is Important [To The ABA] Right Now?

The current crisis within the ABA

Carolyn Y. Forrest

Last November, the ABA began formulating a plan to decrease its general options budget for fiscal year 2017-18 by $10 million, or by a little more than 10%. The austerity measures were prompted by declining annual revenues, which had required the association to dip into its investments.

The ABA's financial advisor cautioned that the ABA's reliance on its investment portfolio for general operations funding resulted in a decline in the portfolio's value of more than 11.5% during the preceding 30 months. If the ABA continued using its investment portfolio at the same rate to support general operations, the ABA would deplete its investment portfolio.

Although the ABA will implement a full complement of measures over several years, the components where lawyers volunteer their time – the ABA's sections, divisions and forums, like our Forum on Communications Law -- will begin feeling their impact in the upcoming fiscal year. The result will be even less ABA financial and administrative support for the ABA entities.

Was it necessary for the ABA to adopt belt-tightening measures? Definitely. Will it hurt all of us? For sure.

To be fair, ABA leadership has been transparent in its discussions about which measures will best achieve its goals of reducing spending with the least impact on ABA entities. Those participating in the development of the plan have already spent numerous hours and sought input from every ABA entity. For example, our Budget Chair Jim Borelli submitted this Forum's objection to a proposal to centralize all ABA travel and meetings functions in one office. We feel that given our Forum's unique needs, and for the continuity of the excellent programs we have run for decades, the Forum is better served by having a dedicated staff person helping with those arrangements. Other ABA entities also objected, and the ABA withdrew the proposal.

But with all the energy ABA staff and leadership have devoted to cost-cutting, it seems that far less time has been devoted to discussing the leading cause of the ABA's declining revenues: the ABA's declining dues-paying membership base. That decline has hit our Forum, hard. (In fact, the Forum's membership committee has initiated several campaigns to reenlist former members and to attract new ones)

However, even our best efforts cannot counter what may be a contributing factor in the ABA's membership drop-off. In recent years, the ABA has seemed, at times, to be disconnected from its members.

An example of the seeming disconnect between the ABA's leadership and its members recently occurred with the May 9, 2017 announcement of the creation of the ABA Board of Governors' Communications Task Force, whose mission was to review the ABA's "editorial policies and practices" for the publications of all ABA entities. The Task Force actually had been created in January 2017 by ABA President Linda Klein, according to the announcement, in response to the ABA's disagreement with this Forum last fall over an article slated to be published in the fall 2016 edition of this Forum's newsletter, *Communications Lawyer* ("CL").

The Task Force's May 9th memo described its genesis as follows: https://www.americanbar.org/content/dam/aba/administrative/communications_law/communications-tf-memo-to-aba-entities-5-9-17.pdf

> "the primary spark for the Task Force review was an incident in the fall of 2016 when many national news organizations – including the New York Times and USA Today – reported that the ABA had decided not to publish ("was censoring") a report prepared by an ABA publishing entity. In the end, the report was published, but many expressed concern about the incident as well as the public perception of the Association generated by the related media reports. The Task Force was formed to consider these concerns and to assess whether any changes to the Association's editorial policies and practices were appropriate."

Despite this Forum's role as the impetus for the Task Force, neither the Forum's leadership nor the CL editors were advised of the formation or the work of the Task Force; nor were we invited to participate. Immediately upon receiving the May 9th memorandum, the Forum reached out to the ABA to ask why no one had advised the Forum or the CL editors of the Task Force and why the Forum's leadership had not been invited to participate. The

Communications Lawyer (ISSN: 0737N7622) is published four times a year by the Forum on Communications Law of the American Bar Association, 321 North Clark St., Chicago, IL 60654-7598 POSTMASTER: Please send address corrections to ABA Service Center, 321 North Clark St., Chicago, IL 60654-7598.

response was that the ABA did not want the "protagonists" from the fall's dispute to participate.

After a five-month review of the ABA's current editorial policy, the May 9th memo set forth the Task Force's recommendation for a revision (or overhauling, depending on your view) of the editorial policy.

The May 9th memo also asked all ABA entities to review the proposed editorial policy and to submit comments *within 10 days* so that a final recommendation could be presented at the then-upcoming ABA Board of Governors meeting.

That hardly allowed us enough time to catch up on the Task Force's closed-door discussion that led to the proposal. Nor did we have sufficient time to reflect with our members on the debate between our Forum and ABA staff that had brought the ABA to this point.

The ABA's dispute with the Communications Lawyer and the Forum

For those who were not following along at the time: CL editors advised ABA staff in September 2016 that it wanted to publish the fall edition of its newsletter in mid-October because the edition would include a couple of timely articles relevant to the upcoming election and our ABA staff agreed to support that goal. Although the edition was ready for publication on October 11, 2016, two days later, ABA staff informed the Forum that CL could not publish a proposed article – submitted by longtime Forum participant Susan Seager -- that labeled then-candidate Trump a "Libel Bully" and a "Libel Loser" to describe his practice of filing meritless suits to silence his critics; suits he almost always lost. And, obviously, it was well within Seager's First Amendment right to express her opinion.

The ABA wanted the article revised to blunt Seager's language. After several days of quickly called conference calls and a flurry of back and forth emails, the ABA's rationale for its unacceptable position boiled down to: (1) concern that Trump might sue the ABA; (2) the ABA's tax-exempt status might be jeopardized because the article could be perceived as a "partisan" attack on Trump; and (3) the article may constitute electioneering in violation of federal regulations.

The Forum's leadership pleaded, then demanded, that the ABA respect our autonomy and the First Amendment, and not cow to the political winds of the moment. After six days of silence, the ABA responded again asking the Forum to make the ABA's proposed, substantive edits. The ABA wanted to strike what it called "ad hominem" Trump attacks and the "tone" of the article. The ABA leadership said publishing the article would "hurt [its] credibility with members" because of the perception that the ABA was aligning with one political party against the other. The email did not give the Forum the option of publishing the article without the ABA-proffered edits.

During the Forum's back and forth with ABA staff, the Media Law Resource Center, a trade association of law firms and media companies, published Seager's article. Meanwhile, the Forum continued to withhold the publication of CL's fall edition.

On October 25, 2016, *The New York Times* ("NYT") reported on the Forum's disagreement with the ABA, quoting from an ABA spokesperson who said (falsely) that the association "had only minor and routine objections to the article's tone." The NYT's article also quoted several members of the CL's editorial board, all of whom are former chairs of this Forum. They unanimously assailed the ABA's censorship and defended the article's publication, without the requested edits, as a well-reasoned, scholarly study that was not legally actionable. Thereafter, a host of media outlets, including *The Daily Show with Trevor Noah, Los Angeles Times* and *Vox,* also reported on the dispute.

Rather than directly speaking with or even contacting the Forum's leadership or CL editors, the ABA issued a press release three days after the publication of the NYT's article (again, falsely) stating that the ABA had never prohibited the Forum from publishing the Trump article and that the proposed edits were merely suggestions. The ABA even requested a retraction from the NYT.

After all of its huffing and puffing, and after the national media resoundingly rebuked the attempted censorship, the ABA relented. On November 3, 2016, the CL fall edition -- with the Trump article included, in its original form -- was published.

Notwithstanding the ABA's handling of the disagreement, the Forum reached out to ABA leadership following the publication of the CL's fall edition to discuss mending the rift and moving forward *together* to accomplish shared goals. The ABA's Deputy Executive Director agreed to attend the upcoming meeting of the Forum's leadership, the Governing Committee.

In the wake of this dismal dispute, the ABA's Deputy Director accepted our invitation and, on November 11, 2016, attended our Governing Committee meeting in Manhattan. He listened as the Forum's leaders detailed their disappointment and frustration with the ABA's handling of the dispute and the ABA's failure to defend the Forum's First Amendment right to publish the article. Forum leaders also urged the ABA to improve its communications with the Forum's leadership. The minutes of that meeting reflect his apology for the ABA's handling of the dispute and the promise that the ABA would learn from this experience and improve the way it handles similar situations in the future.

The Current Debacle

It is therefore regrettable that, a mere two months after the ABA-Forum détente, ABA President Linda Klein would create the Task Force to assess the ABA's editorial policy, but would not invite anyone from the Forum's leadership or CL editors to participate. Moreover, this Forum's leadership is comprised of media attorneys who represent national media outlets and a vast array of publishers. We are uniquely qualified to assist with the Task Force's mission. The ABA's action left some Forum members feeling alienated from the ABA umbrella.

What is interesting about the May 9th memorandum announcing the Task Force is what it says about the Task Force's mission. The mission was

not to assess the "particulars of that incident" in the fall of 2016; nor was it to determine whether the Trump article was good or bad; nor even to decide whether "the actions of those involved were "right" or "wrong"." Instead, the Task Force focused on the ABA's and its entities' "*shared* interest and responsibility *to protect the public perception of the ABA's reputation and brand*" (emphasis added).

With its mission outlined in this way, the Task Force began its review of the ABA's current editorial policy, which had not been fully reviewed since sometime in the 1980s. The Task Force determined that all of the ABA editorial policies recognized two key principles: "(1) the importance of the public image of the ABA that is shaped by its entity publications and (2) the importance of entity control of their publications and editorial content."

To incorporate those principles, the Task Force's proposed ABA editorial policy began with an overarching statement https://www.americanbar.org/content/dam/aba/administrative/communications_law/exhibit-b-aba-proposed-editorial-policy-5-9-17-draft.pdf that, *if* publishing entities comply with the requirements set forth in the ABA editorial policy, *then* they will have the "authority and the responsibility to decide whether and in what circumstances to publish the content that expresses unpopular opinions or encourages controversy."

The proposed editorial policy specifically mandates that every ABA entity adopt its own editorial policy, whereas the Task Force describes the proposed ABA editorial policy as "presenting entities with a more organized "checklist" of points that should be considered in drafting an individual entity's editorial policy." ABA Board of Governors Communications Task Force May 30, 2017 Recommendation for Approval of Revised ABA Editorial Policy. To assist entities in adopting their own policy, the Task Force also urged the ABA to appoint its Standing Committee On Publishing Oversight ("SCOPO") to draft a "template" editorial policy for ABA entities without a policy to use.

Who will decide whether an entity is in compliance with the requirements set out in the ABA's proposed editorial policy? Will it be SCOPO? If an entity believes it is in compliance with the editorial policy and SCOPO disagrees, what is the process for discussing and ultimately resolving the conflict? These questions are left unanswered.

In other words, the proposed policy leaves each ABA entity to decide whether to publish what could be deemed controversial content.

But wait! Does that sound exactly like the situation the Forum faced last fall? It is. And, if ABA leadership disagrees with an entity's decision about specific content, the entity once again will be left to the whims of the then-current ABA leadership. Which ABA leaders ultimately will make the decision? Is there an appeals process? Given what happened last fall, the ABA should have asked the Task Force to deliver a proposal for a process for the resolution of such ABA entity-ABA disagreements over controversial content, with suggestions about who should participate in that process. (This conclusion is not intended to denigrate the work actually performed by Task Force.)

If the ABA's decision truly is to refrain from interfering with an entity's publication of content to which some within the ABA's leadership may object, then why was the Forum singled out in the announcement of the Task Forum?

Because of the importance of an editorial policy, the Forum reviewed the Task Force's proposed revisions, notwithstanding its concerns, and submitted its comments within the ten-day window. https://www.americanbar.org/content/dam/aba/administrative/communications_law/communications-task-force-response-final.pdf

The Forum's comments criticized the ABA for affording practicing attorneys only 10 days for review and consensus-building to review what took the Task Force itself five months to accomplish. The comments also called the ABA to task for excluding the Forum's leadership from participating in the Task Force's work.

In any event, the Forum's comments focused on its substantive concerns. While the requirements set forth in the proposed editorial policy generally are appropriate, the Forum criticized the inclusion of several vague requirements. Each publishing entity must ensure that proposed publications "comply with ABA standards of civility (*see* ABA Resolution 108(1) and (2), August 2011);" (ii) "not engage in partisan political advocacy and not advocate for or against any political candidate or party;" and (iii) not defame or violate the law.

There requirements do not give clear guidance of what constitutes "civility," or "partisan political advocacy," even after reviewing the ABA Resolutions. And what does the ABA mean by "defame" – is that simply a proxy for unflattering but truthful information? Or does the ABA truly believe it needs a policy warning lawyers against committing torts like defamation?

On June 10, 2017, the Board of Governors adopted the revised editorial policy and accepted the Task Force's recommendations, including that every ABA publishing entity adopt its own editorial policy and submit it to SCOPO by June 2018. Following the Board's actions, the Task Force contacted the Forum to advise that the Forum's comments, along with the comments of seven other entities, were reviewed and discussed extensively. However, the Task Force did not recommend any substantive revisions to its version of the proposed editorial policy as a result of any of the comments submitted. The Task Force also invited the Forum to have a representative participate in SCOPO's development of a template for an editorial policy for entities without one.

So in the end, the ABA censored us, mischaracterized its actions in the press, shut us out of a high-level discussion that was prompted by our publication, gave us virtually no time to react to its policy pronouncement, and declined to incorporate any of our input.

The ABA wants, and desperately needs, to encourage ongoing participation by its members, recruitment of new members, and renewed engagement from former members.

Ignoring vibrant components such

as our Forum is not going to help the ABA restore itself to fiscal viability or to relevancy in the bar.

The Myth of Police Officer Privacy

Continued from page 1

information. Nevertheless, in numerous states, general exemptions for "personal privacy" have been cited by police departments, attorneys general, and some courts as the basis for withholding records detailing police officers' official on-duty conduct.[8]

A minority of states' public records statutes expressly exempt from public access certain records of police conduct.[9] Courts in more than a dozen states have deemed records of police conduct to be exempt from public records on these—and other—statutory bases.[10] Those decisions, however, are beyond the scope of this article, which is only concerned with the use of generalized *privacy* exemptions to justify withholding (which the legislatures in those states have already apparently considered in enacting those blanket exemptions).

Using personal privacy exemptions as a basis for denying public access to records of police officers' on-duty conduct badly misconstrues the concept of "personal privacy." First, as set out in the FOI laws, or as interpreted by the courts, FOI exceptions almost always are to be narrowly construed to maximize public access to information.[11] Expanding the "personal privacy" exemptions to withhold information about public servants' on-duty, official activities risks undermining the very purpose of FOI laws: to enable the public to monitor the conduct of official government business.

Second, as discussed below, "personal privacy" has been restricted, in a variety of legal contexts, only to information about individuals (not corporations, associations, or governmental units) that are of a highly personal and "sensitive" nature – such as HIV status, medical or psychological information, or other similar types of information that society recognizes as being subject to an objectively reasonable "expectation of privacy." While compensation and job performance information is considered "private" in the private sector employment context, it is generally accepted that public employees, and especially public officials, must reasonably expect that these data points are not entitled to hidden from public scrutiny.[12] As the Louisiana Court of Appeals held in a well-reasoned decision regarding access to police Internal Affairs Department ("IAD") files under its state freedom of information law, "[a] lthough police officers may have a legitimate privacy interest in certain narrowly circumscribed portions of files concerning their off-duty, private conduct, they do not enjoy a reasonable expectation of privacy with respect to records concerning only how they discharge their official duties."[13]

Similarly, Maryland's intermediate appellate court held that IAD files concerning allegations of racial profiling against state troopers, "do not involve private matters concerning intimate details of the trooper's private life. Instead, such complaints involve events occurring while the trooper is on duty and engaged in public service. As such, the files at issue concern public actions by agents of the State concerning affairs of government, which are exactly the types of material the [Maryland FOI] Act was designed to allow the public to see."[14]

Third, although FOI officers and courts are sensitive to the privacy interests of law enforcement, outside of that specific context, courts have been skeptical of the argument that government employees' personal privacy is a legitimate basis for withholding government records of public-facing official activity.[15]

We believe the better position is that articulated by, for example, the Kentucky Attorney General, that police officers are to be treated like any other public employee:

> A public employee's name, position, work station, and salary are subject to public inspection, as well as portions of the employee's resume reflecting relevant prior work experience, educational qualifications, and information regarding the employee's ability to discharge the responsibilities of public employment. In addition, reprimands to employees regarding job-related misconduct, and disciplinary records generally, have traditionally been treated as open records. . . . Conversely, this office has affirmed agency denial of access to a public employee's home address, social security number, medical records, and marital status on the grounds that disclosure would constitute a clearly unwarranted invasion of personal privacy. Such matters are unrelated to the performance of public employment.[16]

Police personnel records, internal affairs records, or other records of on-duty conduct may differ from other public employees because those records reveal information about law enforcement techniques, confidential informants, national security, or other sensitive law enforcement matters. But other exemptions authorize the withholding of such information, and redaction is the appropriate response, rather than categorical withholding.[17] There is no sound basis for treating law enforcement differently from other public servants when it comes to FOI laws and records of official acts, on duty, especially where they occur in public.

CIVIL RIGHTS CLAIMS BY POLICE OFFICERS

Origins of the Constitutional Right to Informational Privacy

The second context in which "officer privacy" has been raised is where a government agency releases records containing information about police officers' official activities, without the consent of the subject officers. In those circumstances, officers sometimes bring claims against the agency, asserting the unauthorized disclosure violated their constitutional right to privacy.[18] That right arises from two separate sources in our nation's Constitution.

Of course, the word "privacy" does not appear in the U.S. Constitution. Even the Fourth Amendment, which protects persons from unreasonable search and seizure of places, papers, persons, or effects by the government, does not itself include the "private"

modifier. Nevertheless, interpreting that amendment, the United States Supreme Court has recognized that such transgressions can occur only when government agents intrude, unjustifiably, into one's sphere of personal privacy.[19]

The sphere of personal privacy protected by the Fourth Amendment is circumscribed by two necessary conditions: an individual must have an actual, subjective expectation of privacy and that expectation must also be objectively reasonable. Thus, to be entitled to the protections against unwarranted interceptions of communications or the search of one's person, papers or effects, it is not sufficient for the subject of the intrusion subjectively to consider them "private;" they must *also* be the type of materials or activities whose privacy "society is prepared to recognize as reasonable."[20] As the Supreme Court has held, the Fourth Amendment "does not protect all *subjective* expectations of privacy, but only those that society recognizes as 'legitimate.'"[21]

This objective component of the "reasonable expectation of privacy" varies by context, and necessarily incorporates societal norms and mores balanced against other countervailing public interests.[22] Thus, under the "open fields" doctrine, there is no reasonable expectation of privacy in one's real property that is readily visible to the public,[23] and under the "plain view" doctrine, this exception extends to matters that are within the view of a government agent who is lawfully present in a particular "private" location.[24] As demonstrated below, these concepts—rooted in the "search and seizure" context—have been transmuted into the related context of government *disclosure* of information about individuals.

The second "source" of the constitutional "right of privacy" comes not from any specific textual provision of the Constitution, but has been judicially found to arise under the "penumbra" of other rights protected in the Bill of Rights.[25] One aspect of this "right to privacy" is what has been deemed "informational privacy" – the right to control when the government may publicly release private information about private individuals.[26] The Supreme Court first recognized this related area of privacy rights in *Whalen* v. *Roe*, in which recipients of government benefits raised concerns about the gathering of private and personal information by the government, in part, because such information might later be publicly disclosed without the citizen's consent.[27] As the Court put it:

> The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. . . . [I]n some circumstances *that duty arguably has its roots in the Constitution* . . . .[28]

Nevertheless, the Court found that the government's precautions against inadvertent disclosure of "personal and private" information were sufficient; the gathering of highly personal information by government authorities did not violate recipients' right of privacy.[29]

The Supreme Court extended the "right of informational privacy" to public officials in *Nixon v. v. Administrator of General Services,* which involved President Nixon's claim that his own "personal privacy" prevented government disclosure, without his consent, of audio recordings he had made of his conversations in the Oval Office (a/k/a/ "the Nixon tapes").[30]

The Court acknowledged that public officials are not wholly without constitutionally protected privacy rights *in matters of personal life unrelated to any acts done by them in their public capacity*."[31] For example, the Court observed that "matters concerned with family or personal finances" or "private communications between [the President] and, among others, his wife, his daughters, his physician, lawyer, and clergyman" might be legitimately deemed "private" and precluded from public disclosure.[32] This was also the reason given by former Secretary of State Hillary Clinton for withholding many of her email messages that, she asserted, concerned purely private matters, such as planning her daughter's wedding.[33]

The *Nixon* Court drew a bright line between the actions of public officials that are entitled to a "reasonable expectation of privacy" and those that are not. The "overwhelming bulk" of the 42 million pages of documents and the 880 tape recordings at issue in *Nixon* pertained to "the official conduct of [Nixon's] Presidency" and not to private communications or matters.[34] Therefore, the Court concluded "only a minute portion of the materials *implicates appellant's privacy interests*," precisely because "of his *lack of any expectation of privacy* in the overwhelming majority of the materials" – those that reflected on his official conduct.[35]

Application of "Informational Privacy" to Police Officers' Records

Based on these Fourth Amendment principles, and the standards established in *Nixon*, state and federal courts have held that police officers do not have a cognizable privacy interest in records concerning their conduct while on duty—and cannot bring civil claims to prevent disclosure—so long as the records do not contain "highly personal," "intimate," or "sensitive" information.[36] For example, in addition to the information identified in *Nixon*, courts have recognized that the names of police officers' family members, their home addresses, officers' personal employment references, and details of employment prior to entering law enforcement could constitute "private" information—so long as it is irrelevant to official conduct (or misconduct).[37]

Not only are police officers' interactions with members of the public often conducted "in plain view," on public streets, sidewalks and other public thoroughfares (rendering such interactions, by definition, not "private"), they involve the exercise of official police functions. As demonstrated below, time and again, courts throughout the coun-

try have recognized that such activities by sworn peace officers involve inherently "public" functions, the contents of which – whether recorded by video, photography, or discussed in the police department's own investigative files concerning that official conduct – do not involve the officers' "highly personal and sensitive" affairs, and thus are not within the officers' sphere of "*personal* privacy."

STATE COMMON LAW CLAIMS FOR INVASION OF PRIVACY

In drawing the parameters of the public official's "reasonable expectation of privacy" in the disclosure of information maintained *by the government*, courts have also appropriately looked to the related field of "invasion of privacy" committed by *private* actors.[38] Although the precise contours vary, all states recognize at least two distinct, but closely related, civil causes of action for "invasion of privacy" committed by private actors' unjustifiable violation of another's "sphere of personal privacy."

Two Related Causes of Action for "Invasion of Privacy"

The first of these civil tort claims, known as "intrusion upon solitude or seclusion," occurs when one intrudes, without the plaintiff's consent, into an area enshrouded by a "reasonable expectation of privacy."[39] The paradigmatic examples of such places are one's bedroom, hospital room, bathroom, or other similar inherently "private" location.[40] But the tort also has been extended to unconsented to access to *records* containing highly personal and private information, including personal diaries, medical records, and psychological or psychiatric records.[41] The tort is committed upon the "intrusion" into such highly personal and private sphere, without consent or justification, and does not require (or compensate for) damages resulting from further disclosure or publicity given to the private information improperly accessed.

The second independent "invasion of privacy" tort recognized in common law is identified as "unreasonable publicity given to private facts," which provides monetary compensation for another's widespread disclosure of truthful information about an individual that is "private," "personal," and the disclosure of which is deemed "highly offensive to a reasonable person."[42]

These two independent "invasion of privacy" torts share a common requirement: the "sphere of privacy" intruded upon, or the information that was given widespread publicity, must —like the "sphere of personal privacy" protected by the Fourth Amendment against government *intrusion*, and by the Due Process Clauses against governmental *disclosure*—be both subjectively and objectively "reasonable."[43]

Both of these tort claims are therefore subject to two well-recognized exceptions that should also properly apply to records documenting police officers' official conduct: (1) activities occurring in "public" places are not entitled to a reasonable expectation of privacy; and (2) the conduct of public officials, in discharging their official duties (even in "private" places), is not entitled to an objectively "reasonable expectation of privacy."

No Privacy on a Public Street, Sidewalk, Park, Etc.

In contrast to European and other foreign jurisdictions' jurisprudence, in America, it is firmly established that individuals (whether they be royalty, celebrities, or private individuals) do *not* have a reasonable expectation of privacy with respect to their conduct in a public place. Thus, the Restatement (Second) of Torts states that there is no privacy violation when an individual is photographed, without her consent, in public:

> The defendant is subject to liability . . . only when he has intruded into a *private* place, or has otherwise invaded a *private* seclusion that the plaintiff has thrown about his person or affairs. Thus, there is no liability . . . . for observing him or even *taking his photograph* while he is walking on the public highway, since he is not then in seclusion and his appearance is public and *open to the public eye*.[44]

Under this rule of law, a "public place" includes not only streets, parks, or other publicly-controlled locations, but also businesses and other private properties that are generally open to the public.[45]

As the Supreme Court of Washington put it, "[o]n the public street or in any other public place, the plaintiff has no legal right to be alone; and it is no invasion of his privacy to do no more than follow him about and watch him there."[46] The court went on to explain that because an individual in public has no expectation of privacy, there also is no right to privacy in a recording or "full written description[ ] of a public sight which anyone would be free to see."[47]

These principles have been applied specifically to police officers in the context of citizens photographing and recording police officers in public. A police officer, like any other citizen, has no common law right to privacy from members of the public recording those activities or writing accounts of what they have observed. For example, in *Glick v. Cunniffe*, the First Circuit affirmed that private citizens have the right to record video and audio of public officials performing their official duties in a public place.[48] Similarly, in *Johnson v. Hawe*, the Ninth Circuit held there was no expectation of privacy where a police officer was videotaped sitting in an open vehicle, talking on a cellphone where members of the public could hear him.[49]

The logic of those decisions applies with equal force to *records* documenting, memorializing, or discussing a police officer's conduct in a public place. Police conduct—and even more so alleged *mis*conduct—often involves police activities in public places or, to the extent that it occurs on private property or inside a police station, within "plain view" of members of the public. It would defy logic for the recordings that were made in *Glick* or *Johnson* to be deemed "private" simply because they were created by the police, or were filed by citizens as part of a complaint against the officers, or because they became relevant to an internal affairs investigation.[50] Where there is no privacy in the underlying conduct itself, there cannot be a privacy interest in recordings of that same conduct.

No Expectation of Privacy in A Public

Official's Discharge of His or Her Official Duties

With respect to the "publicity given to private information" tort, the courts have limited the scope of protected information to material of a "highly personal and sensitive" nature about individuals (such that it's public disclosure "would be offensive and objectionable to a reasonable person.")[51] Information and materials that have been found to meet this standard include, for example, a person's HIV status,[52] or psychiatric or psychological treatment records.[53]

In contrast, numerous courts have held that information contained in records regarding police officers' performance of their official duties is *not* the type of "highly personal and sensitive" material that is appropriately deemed "private". For example, the Tenth Circuit repeatedly has held that "police internal investigation files [are] not protected by the right to privacy when the 'documents related simply to the officers' 'work as police officers.'"[54]

The Washington State Supreme Court similarly reasoned that:

In contrast to the types of information listed in the Restatement's comment [b], the information contained in the police investigatory reports . . . does not involve private matters, but does involve events which occurred in the course of public service. Instances of misconduct of a police officer while on the job are not private, intimate, personal details of the officer's life . . . . They are matters with which the public has a right to concern itself.[55]

Similarly, West Virginia's Supreme Court has held that disclosure of "conduct by a state police officer while the officer is on the job in his or her official capacity as a law enforcement officer and performing such duties, including but not limited to, patrolling, conducting arrests and searches, and investigating crimes" is not an invasion of that officer's right to privacy.[56] Numerous other courts, in a variety of jurisdictions, have reached the same conclusion.[57]

While police officers occupy a special role in our society, making the public's interest in their discharge of official duties perhaps more compelling than is true of other public servants, this rule is by no means unique to law enforcement. Courts across the country have found that public officials, in a variety of settings, can claim no "legitimate" or "reasonable" expectation of privacy with respect to records that memorialize or evaluate their performance of official governmental duties. For example, the Alaska Supreme Court ordered disclosure of performance evaluations of the head of the Anchorage public libraries, rejecting the claim that the official had a privacy interest in the information.[58] The court emphasized that there is a presumption that "public officials are properly subject to public scrutiny in the performance of their duties."[59] Further, "the performance evaluation did not in any way deal with the personal, intimate, or otherwise private life of [the official]."[60] Courts in a variety of jurisdictions have reached similar conclusions regarding records reflecting public officials' job performance.[61]

Applying this same rationale, several states courts have held it is not an invasion of privacy to disclose the performance evaluations of public school teachers.[62] In New York in 2010, for example, a teachers' union petitioned to keep the Department of Education from publicly releasing individual "Teacher Data Reports."[63] The court concluded that releasing the reports "would not be an 'unwarranted' invasion of privacy since the data at issue relates to the teachers' work and performance and is intimately related to their employment with a city agency and does not relate to their personal lives."[64] The court emphasized that "Courts have repeatedly held that release of job-performance related information, even negative information such as that involving misconduct, does not constitute an unwarranted invasion of privacy."[65] This was in contrast to "releasing personal information such as birth dates and personal contact information such as email addresses of state employees," which could constitute an unwarranted invasion of personal privacy.[66]

To the extent that police IAD records *do* contain discreet pieces of truly "highly personal and sensitive" information (e.g., home address, phone number, or social security numbers, the identities of undercover agents or confidential informants), redaction of such information is the appropriate remedy, not categorical withholding of police records.[67] As the Colorado Supreme Court said, in a case involving the IAD file of a deputy sheriff:

By providing the custodian of records with *the power to redact names, addresses, social security numbers, and other personal information*, disclosure of which may be outweighed by the need for privacy, the legislature has given the custodian [of such records] an effective tool *to provide the public with as much information as possible*, while still protecting privacy interests when deemed necessary.[68]

The Countervailing Public Interest in Disclosure and Transparency

As noted above, the scope of information entitled to an objectively "reasonable expectation of privacy" necessarily incorporates a balancing of the individuals' desire for confidentiality/secrecy and society's interest in having access to that information. Accordingly, the "publicity given to private facts" tort is frequently limited to disclosure of information in which there is no legitimate public interest. Indeed, the Restatement of Torts recognizes that public figures and public officials do not, by virtue of their status, relinquish all claims to a right of privacy. However, in recognition of the public's constitutionally-based right to receive information about public officials (and other persons of significant public interest), the Restatement states that:

The line is to be drawn when the publicity ceases to be the giving of information to which the public is entitled, and becomes a morbid and sensational prying into private lives for its own sake, with which a reasonable member of the public, with decent standards, would say that he had no concern.[69]

This is perhaps the underlying reason why documents (photos, videos,

and written records) that depict or describe and analyze a police officer's discharge of official duties is deemed to be inherently "public" and not "private." As the United States Supreme Court has recognized, "[t]he public . . . has a strong interest in exposing *substantial allegations* of police misconduct to the salutary effects of public scrutiny."[70] And even apart from allegations of misconduct, "the conduct of a policeman on duty is legitimately and necessarily an area upon which public interest may and should be focused."[71]

As one court put it, "[t]here is perhaps no more compelling justification for public access to documents regarding citizen complaints against police officers than preserving democratic values and fostering the public's trust in those charged with enforcing the law."[72] Similarly, in a strident decision granting public access to records produced in discovery, the court in *Doe v. Marsalis*[73] assessed claims of police privacy in internal police records alleging on-duty sexual misconduct by Chicago police found them grossly outweighed by the importance of public oversight of the police. "Police misconduct creates one of the ultimate 'lose/lose' situations in our democratic society," the court wrote, noting that it has "multiple layers of victims," from the individual directly injured to the police department itself, to the public at large. "The only way to end this syndrome is to evaluate and reevaluate past practices. . . . Some of these issues require public debate and appropriate media scrutiny."[74] The court noted the positive impact of previous media scrutiny and concluded, "Clearly, if Defendant's confidentiality position were adopted by this Court, these types of articles could never be written and public debate would suffer."[75]

OTHER SOURCES

In addition to the case law discussed above, several professional associations of law enforcement agencies and officers have recognized that claiming "officer privacy" to withhold photos, videos or records discussing the official actions of particular officers on a given occasion, and those records showing how the department investigated that conduct, erodes the public trust and thereby ultimately undermines the effectiveness of law enforcement.

Responding to a string of high-profile police shootings of African American men and the riots that followed, on December 18, 2014, President Barack Obama signed an executive order establishing the Task Force on 21st Century Policing. Among its major recommendations was to "establish a culture of transparency and accountability in order to build public trust and legitimacy."[76]

Following a three-day Conference on Public Trust that brought together dozens of senior law enforcement officials from across the country, the Major County Sheriffs' Association, along with the FBI's National Executive Institute Associates, issued a report, "Public Trust: A Shared Responsibility." That report identified two noteworthy "Factors Contributing to Public's Distrust of Police":

> • No accountability for law enforcement officers' actions.
>
> • Lack of transparency by police.[77]

The conference report included the following "Action Strategies for Building Public Trust":

> The public will usually be more supportive of the police when they are upfront in acknowledging mistakes and providing the appropriate response. Covering up an incident or withholding information is totally unacceptable in today's transparent atmosphere.[78]

Perhaps most important, the conference report also noted that "Police Officers' Bill of Rights interferes with being transparent."[79]

The International Association of Chiefs of Police has also published this recommendation concerning incidents that give rise to internal affairs investigations and the imposition of discipline:

> **Ensure transparency and accountability when incidents do happen.** Share what can be shared—and do it quickly. Provide as much information as possible to internal affairs investigations. Often, regardless of the original situation or decision made, **if the chief clearly communicates what happened**–why police took a particular action; basis for its procedures; and **any disciplinary actions taken – trust can be established and sustained. The department's response to an incident can be as, or more, impactful than the original incident in sustaining trust.** [80]

CONCLUSION

We readily acknowledge that myriad situation-specific reasons justify withholding particular photos, video recordings, and documents concerning official police conduct: the disclosure of certain details in such records could compromise an ongoing investigation, expose the identities of undercover agents, or place certain officers and/or third parties in physical danger or threaten their personal safety. We do not suggest that eliminating "officer privacy" as a basis for denying access will render *all* police records, *in their entirety* automatically subject to inspection

Our thesis is far more modest: it is high time to acknowledge that "police officer privacy" – at least when it comes to records concerning the discharge of peace officers' official duties – is a myth, *not* a legitimate basis on which to deny public access to such records As the Illinois Court of Appeals put it:

> The conduct of a policeman on-duty is legitimately and necessarily an area upon which public interest may and should be focused. . . . [T]he very status of the policeman as a public official . . . is tantamount to an implied consent to informing the general public by all legitimate means regarding his activities in discharge of his public duties.[81]

Endnotes

1. *See, e.g.,* Associated Press, *Pueblo Police Officer Accused of Re-Enacting Body Cam Footage Will Be Disciplined*, The Denver Post, (Jun. 3, 2017), http://www.denverpost.com/2017/06/02/pueblo-police-officer-re-enacting-body-camera-footage (reporting significant alleged misconduct by an officer but noting that "the extent of his punish-

ment will not be released because the matter is a personnel investigation."); Muckrock, *Amherst Police Dept. Response to Public Records Request* (Sept. 21, 2016) https://www.muckrock.com/foi/amherst-2/internal-affairs-files-28160/.

2. *See, e.g.,* Catherine Green, *There's Still Not Much Transparency Surrounding Those Transparency-Boosting Body-Cameras*, Voice of San Diego (Jun. 11, 2015) (noting that a California State Senator mentioned, among factors to consider in legislation governing access to body-worn camera footage "privacy of officers"), available at http://www.voiceofsandiego.org/topics/public-safety/theres-still-not-much-transparency-surrounding-those-transparency-boosting-body-cameras/.

3. *See, e.g.*, *Johnson v. Hawe*, 388 F.3d 676 (9th Cir. 2004).

4. *See, e.g.*, Ala. Code § 36-12-40; Ariz. Rev. Stat. Ann. §§ 39-121 - 39-128 & 38-1109; Fla. Stat. §§ 112.533(2)(a) & 119; Ga. Code Ann. § 50-18-72(a)(8); Haw. Rev. Stat. § 92F-14.

5. *See, e.g.*, Cal. Penal Code § 832.7 (2007); Neb. Rev. Stat. 84-712.95 (2007); S.D. Codified Laws § 1-27-1.5(7); Vt. Stat. Ann. tit. 20, § 1923.

6. *E.g.*, Alaska Stat. Ann. §§ 40.25.120 (access may be denied if disclosure would constitute an "unwarranted invasion of . . . privacy") & 39.25.080; Ark. Code Ann. § 25-19-105(c)(1) (police disciplinary records not public unless they pertain to an officer's suspension or termination and there is a "compelling public interest" in disclosure); Conn. Gen. Stat. § 1-210 (police disciplinary records exempt if they would constitute "an invasion of personal privacy.").

7. *See, e.g.*, 5 U.S.C. §§ 552(b)(6) & (7); N.Y. Pub. Off. §§ 89.2-89.2-a.

8. *See supra* n.1; *infra* nn.13-14, 16-17; *Bolm v. Custodian of Records of Tuscon Police Dept.*, 193 Ariz. 35 (Az. Ct. App. 1998) (affirming denial of access to IAD records in their entirety on grounds of confidentiality and privacy).

9. *See, e.g.*, *supra* n.5.

10. *See* J. R. Macht, "Should Police Misconduct Files be Public Record? Why Internal Affairs Investigations and Citizen Complaints Should be Open to Public Scrutiny," 45 No. 6 Crim. Law Bull. nn. 26-27 (2009) (collecting cases and statutes); WNYC-FM, *Is police misconduct a secret in your state?* (Oct. 15, 2015), available at http://www.wnyc.org/story/does-public-have-right-police-personnel-records/ (50-state guide to access to police IA investigations). Many FOI laws also exempt public employees' "personnel files" or records of criminal investigations, which have been used as an alternative basis for withholding police officers' records. *See, e.g.*, *State v. Garrison*, 711 N.W.2d 732 (Table) (Iowa Ct. App. 2006); *Union Leader Corp. v. Fenniman*, 620 A.2d 1039 (N.H. 1993).

11. *See, e.g.*, *Dep't of Interior v. Klamath Water Users Protective Ass'n*, 532 U.S. 1, 8 (2001).

12. *See, e.g.*, *Int'l Fed'n Of Prof'l and Tech. Eng'rs*, *Local 21, AFL-CIO v. Superior Ct.*, 165 P.3d 488 (Cal. 2007); *Municipality of Anchorage v. Anchorage Daily News*, 794 P.2d 584, 591 (Alaska 1990).

13. *City of Baton Rouge v. Capital City Press, LLC*, 4 So. 3d 807, 821 n.19 (La. Ct. App. 2008) (citations omitted), *modified on rehearing,* 7 So. 3d 21 (La. Ct. App. 2009).

14. *Maryland Dep't of State Police v. Maryland State Conference of NAACP Branches*, 988 A.2d 1075, 1080 (Md. Ct. Special App. 2010), *aff'd,* 59 A.3d 1037 (Md. 2013). The Maryland Court of Appeals subsequently narrowed its ruling to apply only to the release of anonymized internal affairs files, a position that, as set out in this article, we believe is erroneous.

15. *See, e.g.*, *infra* nn. 58-64.

16. Opinion of the Office of the Attorney General of Kentucky, 03-ORD-213 (Oct. 10, 2003) at *3-4 (quotation and citations omitted), *ag.ky.gov/civil/civil-enviro/orom/2003/03ORD213.doc*.

17. *City of Baton Rouge v. Capital City Press, LLC*, 7 So. 3d 21, 23 (La. Ct. App. 2009) (ordering production of IAD records redacted to remove home addresses, telephone numbers, social security numbers, and medical information *except* "medical information that is related to the alleged officer misconduct at issue.").

18. *See, e.g.*, *Flanagan v. Munger*, 890 F.2d 1557 (10th Cir. 1989); *Kallstrom v. City of Columbus*, 165 F. Supp. 2d 686, 695 (S.D. Ohio 2001); *Int'l Fed'n Of Prof'l and Tech. Eng'rs*, 165 P.3d 488.

19. *Katz v. United States*, 389 U.S. 347 (1967).

20. *Katz,* 389 U.S. at 361 (Harlan, J., concurring). *See also Kyllo v. United States*, 533 U.S. 27, 34 (2001) (reaffirming the applicability of "[t]he *Katz* test").

21. *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995) (emphasis added) (citation omitted).

22. *Veronia Sch. Dist. 47J*, 515 U.S. at 654; J. Thomas McCarthy, *Rights of Publicity and Privacy* § 5:98 (2d ed. 2010) (recognizing that the zone of privacy "that is legally protected is dependent upon both the social customs and norms which govern a given context") (citation omitted).

23. *Hester v. United States*, 265 U.S. 57, 57 (1924); *Oliver v. United States*, 466 U.S. 170, 179 (1984).

24. *Horton v. California*, 496 U.S. 128 (1990).

25. *See Griswold v. Connecticut*, 381 U.S. 479, 483-84 (1965); *Roe v. Wade*, 410 U.S. 113, 152-53 (1972) (collecting cases).

26. *See* Timothy Azarchs, *Informational Privacy: Lessons From Across the Atlantic*, 16 U. Pa. J. Const. L. 805 (2014).

27. 429 U.S. 589 (1977).

28. *Whalen*, 429 U.S. at 605 (emphasis added).

29. *Id.* at 605-06.

30. 433 U.S. 425 (1977).

31. *Id.* at 457 (emphasis added).

32. *Id.* at 457-59.

33. Zeke Miller, *Hillary Clinton Did Not Keep Personal Emails*, TIME, Mar. 10, 2015.

34. *Id.* at 459.

35. *Id.* at 461-65.

36. *See e.g., Flanagan*, 890 F.2d 1557; *City of Loveland v. Loveland Publ'g Corp.*, No. 03 CV 513, 2003 WL 23741694, at *3 (Colo. Dist. Ct. June 16, 2003); *Cowles Publ'g Co. v. State Patrol*, 748 P.2d 597 (Wash. 1988).

37. *See, e.g.*, *Charleston Gazette v. Smithers*, 752 S.E.2d 603, 619 (W. Va. 2013); *City of Baton Rouge*, 7 So.

3d at 23; *City of Loveland*, 2003 WL 23741694, at *3; *Puzick v. City of Colo. Springs*, 680 P.2d 1283, 1287 (Colo. Ct. App. 1983).

38. *See State of Hawai'i Org. of Police Officers v. Soc'y of Prof'l Journalists-Univ. of Hawai'i Chapter*, 927 P.2d 386, 406 (Haw. 1996) (collecting cases), *superseded by statute as recognized in Peer News LLC v. City & Cty. of Honolulu*, 376 P.3d 1 (Haw. 2016).

39. *See* Restatement (Second) of Torts § 652B (1977). *See also* Eli A. Meltz, *No Harm, No Foul? "Attempted" Invasion of Privacy and the Tort of Intrusion Upon Seclusion*, 83 Fordham L. Rev. 3431, 3440-43 (2015).

40. *See, e.g.*, *Hamberger v. Eastman*, 206 A.2d 239 (N.H. 1964); *Kohler v. City of Wapakoneta*, 381 F. Supp. 2d 692 (N.D. Ohio 2005); *Shulman v. Group W Prods., Inc.*, 955 P.2d 469 (Cal. 1998); *Noble v. Sears, Roebuck & Co.*, 109 Cal. Rptr. 269 (Cal. Ct. App. 1973).

41. *See, e.g.*, Restatement (Second) of Torts § 652B cmt. b (intrusion need not be physical); *Shulman* 955 P.2d at 469 (intrusion extends to data); *Ferguson v. City of Charleston*, 532 US. 67, 78 (2001); *Mason v. Stock*, 869 F. Supp. 828, 833 (D. Kan. 1994).

42. Restatement (Second) of Torts § 652D.

43. *See, e.g.*, Restatement (Second) of Torts § 652B; *Shulman*, 955 P.2d at 469; *Citizens to Recall Mayor James Whitlock v. Whitlock*, 844 P.2d 74, 77 (Mont. 1992).

44. § 652B cmt. C (1977) (emphases added). *See also Salazar v. Golden State Warriors*, No. C-99-4825, 2000 WL 246586, at *2 (N.D. Cal. Feb. 29, 2000); *I.C.U. Investigations, Inc. v. Jones*, 780 So. 2d 685 (Ala. 2000); *Shulman*, 955 P.2d at 490.

45. *See, e.g.*, *Med. Lab. Mgmt. Consultants v. ABC*, 306 F.3d 806, 812-15 (9th Cir. 2002); *People v. Corley*, 2001 WL 1359530, at *5 (N.Y. Sup. Ct. Aug. 7, 2001)).

46. *Mark v. Seattle Times*, 635 P.2d 1081, 1094 (Wash. 1981) (citation omitted).

47. *Id.*

48. 655 F.3d 78 (1st Cir. 2011).

49. 388 F.3d 676 (9th Cir. 2004).

50. That is, however, an argument that some police departments have made. *See, e.g.*, *Cox v. New Mexico Dep't of Pub. Safety*, 242 P.3d 501, 507 (N.M. Ct. App. 2010) (rejecting law enforcement argument that civilian complaints are "private").

51. *Martinelli v. Dist. Ct. In and For City and Cty. of Denver*, 612 P.2d 1083, 1091 (Colo. 1980). *See also Flanagan,* 890 F.2d at 1570.

52. *Doe v. High-Tech Inst., Inc.*, 972 P.2d 1060 (Colo. Ct. App. 1998).

53. *Kerns v. Bader*, 663 F.3d 1173, 1198 (10th Cir. 2011) (noting that "[p]sychiatric records have been afforded even greater protection" than medical records, when it comes to privacy); *Mason v. Stock,* 869 F. Supp. 828, 833 (D. Kan.1994) (psychological records are the only items in police officers' personnel files that are "so highly personal and sensitive" that they are within the constitutional zone of privacy).

54. *Stidham v. Peace Officer Standards And Training*, 265 F.3d 1144, 1155 (10th Cir. 2001) (quotation omitted). *Accord Mangels v. Pena*, 789 F.2d 836, 839 (10th Cir. 1986) (rejecting a claim of privacy in police internal affairs investigation files; "the legitimacy of an individual's expectations [of privacy] depends . . . upon the intimate or otherwise personal nature of the material which the state possesses," and the performance of official duties is not of such a nature); *Denver Policemen's Protective Ass'n v. Lichtenstein*, 660 F. 2d 432, 435 (10th Cir 1981) (police officers have no legitimate privacy interest in "documents related simply to the officers' work as police officers.").

55. *Cowles Publ'g Co.*, 748 P.2d at 605. *Accord Romero v. City of Fountain*, 307 P.3d 120, 125 (Colo. Ct. App. 2011) (refusing to stay public release of an IAD file pending appeal, because this was information which "the public would have the right to know . . . .").

56. *Charleston Gazette v. Smithers*, 752 S.E.2d 603, 619 (W. Va. 2013).

57. *See, e.g.*, *Zaffuto v. City of Hammond*, 308 F.3d 485, 490-91 (5th Cir. 2002) (no legitimate expectation of privacy in phone conversations discussing only police department policies); *Kallstrom*, 165 F. Supp. 2d at 695 (no privacy interest in disciplinary records, incident complaints from citizens, and other documents detailing how each officer is performing); *Smithers*, 752 S.E.2d at 619; *State of Hawai'i Org. of Police Officers*, 927 P.2d at 407; *Great Falls Tribune Co. v. Cascade Cty. Sheriff*, 775 P.2d 1267, 1269 (Mont. 1989); *City of Baton Rouge v. Capital City Press, LLC*, 4 So.3d 807 (La. Ct. App. 2008).

58. *Municipality of Anchorage*, 794 P.2d at 591.

59. *Id.*

60. *Id.*

61. *See, e.g.*, *Deseret News Publ'g Co. v. Salt Lake Cty.*, 182 P.3d 372 (Utah 2008); *Capital City Press v. E. Baton Rouge Parish Metropolitan Council*, 696 So. 2d 562, 567 (La. 1997); *Whitlock*, 844 P.2d at 77-78; *Rawlins v. Hutchinson Publ'g Co.*, 543 P.2d 988, 993 (Kan. 1975).

62. In response to these decisions, many states passed legislation specifically exempting teacher evaluations from FOI laws.

63. *Mulgrew v. Bd. of Educ. of City Sch. Dist. of City of N.Y.*, 919 N.Y.S.2d 786, 790 (N.Y. Sup. Ct. 2011), *aff'd,* 87 A.D.3d 506 (N.Y. App. Div.).

64. *Id. Accord Herald Co., Inc., v. Ann Arbor Pub. Sch.*, 568 N.W.2d 411, 414-15 (Mich. Ct. App. 1997) (requiring disclosure of a memorandum of teacher work performance).

65. *Id. See, e.g.*, *Capital Newspapers Div. of Hearst Corp. v. Burns*, 496 N.E.2d 665 (N.Y. 1986) (sick days taken by individual police officer); *Anonymous v. Bd. of Educ. for Mexico Cent. Sch. Dist.*, 162 Misc. 2d 300 (N.Y. Sup. Ct. 1994) (settlement agreement resolving teacher disciplinary charges); *Rainey v. Levitt*, 525 N.Y.S.2d 551 (N.Y. Sup. Ct. 1988) (individuals' scores on civil service exam); *Faulkner v. Del Giacco*, 529 N.Y.S.2d 255 (N.Y. Sup. Ct. 1988) (names of prison guards accused of impropriety); *Farrell v. Village Board of Trustees*, 372 N.Y.S.2d 905 (N.Y. Sup. Ct. 1975) (written reprimands of police officers, including names).

66. *Id.*

67. *See, e.g.*, *City of Baton Rouge*, 7 So. 3d at 23 (ordering the production of internal affairs records redacted to remove home addresses, telephone

numbers, social security numbers).

68. *Freedom Colo. Info., Inc. v. El Paso Cty. Sheriff's Dep't*, 196 P.3d 892, 900 n.3 (Colo. 2008) (emphasis added).

69. Restatement (Second) of Torts § 652D cmt. h.

70. *Waller v. Georgia*, 467 U.S. 39, 47 (1984) (emphasis added).

71. *Cassidy v. ABC*, 377 N.E.2d 126, 132 (Ill. Ct. App. 1978).

72. *Jones v. Jennings*, 788 P.2d 732, 738-39 (Alaska 1990).

73. 202 F.R.D. 233 (N.D. Ill. 2001).

74. *Id.* at 238.

75. *Id.*

76. Final Report of the President's Task Force on 21st Century Policing, at 12 (2015), https://cops.usdoj.gov/pdf/taskforce/taskforce_finalreport.pdf.

77. Major Counties Sheriffs' Ass'n, Public Trust: A Shared Responsibility (2015), http://www.mcsheriffs.com/pdf/news/public_trust_final_4416.pdf.

78. *Id.* at 22-23.

79. *Id.* at 15.

80. Int'l Ass'n Chiefs of Police, IACP National Policy Summit on Community-Police Relations: Advancing a Culture of Cohesion and Community Trust at 21-22 (2015), http://www.theiacp.org/Portals/0/documents/pdfs/CommunityPoliceRelationsSummitReport_web.pdf (emphasis added).

81. *Cassidy*, 377 N.E.2d at 132.

Courts Split on Whether ADA Applies to Websites, as Litigation Continues to Rise

BY GONZALO E. MON AND CRYSTAL N. SKELTON

Since January 2015, more than 450 lawsuits have been filed alleging that companies' websites and/or mobile applications violate the Americans with Disabilities Act (the "ADA") when they are not accessible to the blind. These lawsuits have targeted major retailers, restaurants, hospitality providers, movie theaters, movie and game rental chains, dating services, banks, insurance providers, casinos, and even performing arts centers. No one is safe.

In the past several months, courts have rendered inconsistent decisions concerning whether websites are considered places of public accommodation covered by Title III of the ADA. Meanwhile, the Department of Justice (the "DOJ") has continued to delay its long-awaited regulations on the matter. This has put companies in a difficult position, and has often left them facing threats from various plaintiffs' firms as they try to sort things out.

ADA Overview

Title III of the ADA makes it unlawful to discriminate against the disabled in the full and equal enjoyment of the goods and services of any place of public accommodation by any person who owns, leases (or leases to), or operates a place of public accommodation."[1] Title III identifies 12 specific categories of public accommodations, including (1) clothing stores, grocery stores, other sales or rental establishments; (2) banks, beauty shops, travel services, gas stations, or other service establishments; and (3) restaurants, bars, or other establishments serving food or drink.[2]

It is unlawful both to deny the disabled the opportunity to participate in programs or services and to provide the disabled with separate, but unequal, goods and services. To ensure the disabled have full and equal enjoyment of the goods and services of places of public accommodation, the ADA also requires companies to make certain "reasonable modifications," such as by providing auxiliary aids, to ensure effective access.

The ADA permits any person who is subject to discrimination on the basis of disability in violation of Title III to file a civil action for a permanent or temporary injunction, restraining order, or other order. The prevailing party in such action is entitled to recover a "reasonable" attorney's fee, including litigation expenses and costs. All 50 states and the District of Columbia have also enacted statutes designed, in some form, to protect disabled persons against unlawful discriminatory practices. Certain state laws specify that any violation of the ADA is considered a civil rights violation and violators are subject to a minimum statutory penalty per access violation, plus attorneys' fees. In other states, though, plaintiffs are only entitled to injunctive relief and attorney's fees.

Plaintiffs Target "Commercial" Websites

When the ADA was enacted in 1990, the Internet was in its nascent stage. Traditionally, the ADA was thought to apply only to brick-and-mortar stores, and courts historically were not receptive to the idea that the Internet constitutes a place of public accommodation subject to the requirements of Title III. Nevertheless, since at least the late 1990s, the National Federation for the Blind ("NFB") and other consumer groups have pushed various companies to ensure their websites and other streaming media are accessible to those with disabilities.

Litigation relating to website accessibility really kicked off in 2006, following the NFB's lawsuit against Target over the inaccessibility of its website. NFB's legal theory was that unequal access to Target.com denies the blind the full enjoyment of the goods and services offered at Target stores, which are places of public accommodation.[3] Target moved to dismiss the complaint for failure to state a claim, alleging that the ADA covers access to only physical spaces and not websites, and plaintiffs failed to assert they were denied access to Target stores.

In denying Target's motion to dismiss, the district court in the Northern District of California found that the ADA could apply where there was a "nexus" between the use of the website and enjoyment of the goods and services offered at the retailer's physical store. Moreover, the court found that the services on the Target.com website were "heavily integrated with the brick and mortar stores and operate[d] in many ways as a gateway to the store."[4] The Target decision marked the first time a federal district judge ruled that Title III applies to websites when they act as a gateway to a brick-and-mortar store.

The suit settled in 2008, with Target agreeing to pay over $6 million to the class and $20,000 to a nonprofit corporation dedicated to helping the blind. In addition, Target agreed to make various changes to its website to ensure that "blind guests using screen-reader software may acquire the same information and engage in the same transactions as are available to sighted guests with substantially equivalent ease of use."

Although most cases have involved companies with physical locations, not all have. For example, in 2015, a federal court in Vermont held that Scribd, Inc. — an online-only publishing platform hosting digital books and documents supplied by third parties (and which sells no physical products) — violated Title III of the ADA because its website and mobile apps use "an exclusively visual interface that is inaccessible to

Gonzalo Mon *is a partner in Kelley Drye's Washington, D.C., office.* **Crystal Skelton** *is an associate in the firm's Los Angeles office.*

the blind because they use an exclusively visual interface and lack any non-visual means of operation."[5] Specifically, the court found that Scribd violated the ADA because its website and apps were not programmed to be accessible through screen reader software. The court reasoned that Title III's reference to a "place of public accommodation" is ambiguous and that, as "a remedial statute," the ADA ought to be reviewed liberally in the plaintiff's favor.

Not all courts have been unanimous in this area, however. For example, cases stemming from courts in the Ninth Circuit have decided that an online-only business is not considered a place of public accommodation under the ADA, and is therefore not required to have an accessible website.[6] Although there may still be some gray areas about the application of the ADA to certain websites, the findings in *Target*, *Scribd*, and other cases have led many business to settle cases, rather than litigate them.

DOJ Delays Regulation of Website Accessibility

As the primary enforcer of the ADA, the DOJ could clear up much of this confusion. Over the years, the DOJ has taken the position that Title III covers access to websites of public accommodations, as evidenced through rulemaking efforts, public statements, and recent settlements. However, the agency has not issued any formal regulations.

For nearly a decade, the DOJ has contemplated promulgating a rule to address the applicability of the ADA to private retailers offering goods and services to the public online. Specifically, the DOJ has sought to issue a proposed rule to "make clear to entities covered by the ADA their obligations to make their Web sites accessible." The DOJ's rulemaking has been delayed several times, and the DOJ most recently designated the proposed rule as a 'long term action' of the agency. This likely means that companies will not be seeing a rulemaking for website accessibility applicable to public accommodations under Title III until at least 2018 or, more likely, 2019 or beyond, especially given the change in Administration.

Nonetheless, the DOJ has remained active with its enforcement of website accessibility under Title III of the ADA. For example, in March 2014, the DOJ entered a consent decree with H&R Block, Inc., one of the largest tax return preparers in the U.S., requiring the company to ensure that its website, tax filing utility, and mobile apps are accessible. In November 2014, the DOJ also announced a settlement with Peapod, LLC, an exclusively online business offering a website and mobile app for online grocery shopping and delivery services.

Recent Litigation and Other Developments

Over the past few years, the world of website accessibility has changed dramatically. Whereas we had previously seen a handful of lawsuits filed each year, now we are seeing hundreds of them. To be exact, more than 450 lawsuits have been filed since January 2015. The majority of those suits involve retailers with brick-and-mortar stores selling their goods or service online,[7] but some involve online-only sites or services[8] and even mobile applications.[9]

Although most of these cases are pending or settling, courts have issued a few notable decisions, which underscore how much confusion still exists in this area.

Colorado Bag N' Baggage (California): In March 2016, a California state court granted summary judgment in a case alleging that the Colorado Bag N' Baggage website violated the ADA because it contained numerous access barriers preventing blind and other visually-impaired individuals from gaining equal access to the website. In its order, the court noted that the plaintiff had "presented sufficient evidence and legal argument to conclude Title III of the ADA applies to plaintiff's use of a website where plaintiff has demonstrated he sought goods and services from a place of public accommodation because he demonstrated a sufficient nexus exists between defendant's retail store and its website that directly affects plaintiff's ability to access goods and services." Further, the plaintiff had "presented sufficient evidence that he was denied full and equal enjoyment of the goods, services, privileges, and accommodations offered by [the retailer] because of his disability." The court ordered the company to make its website accessible.

Bang & Olufsen (Florida): Almost one year later, in February 2017, a Florida court issued an opinion finding that "a website that is wholly unconnected to a physical location is generally not a place of public ADA under the ADA."[10] The lawsuit alleged that the retailer violated the ADA because its website is not compatible with screen reader software. The sole issue before the court was whether the website was a place of public accommodation, subject to the ADA. Importantly, the court held that the "ADA does not require places of public accommodations to create full-service websites for disabled persons. In fact, the ADA does not require a place of public accommodation to have a website at all. All the ADA requires is that, if a retailer chooses to have a website, the website cannot impede a disabled person's full use and enjoyment of the brick-and-mortar store."

Domino's (California): In March 2017, another California court agreed that a website could be subject to the ADA, but stopped short of requiring a company to make changes to its website. In that case, Domino's argued that the court should dismiss or stay the action because the DOJ has not promulgated concrete guidance regarding the accessibility standards.[11] The company noted that although the DOJ issued a Notice of Proposed Rulemaking in 2010, it acknowledged that "clear guidance on what is required under the ADA does not exist." Dominos argued that, in the absence of clear guidance, the plaintiff's "request to impose liability under the ADA for Defendant's alleged failure to abide by certain accessibility standards would violate Defendant's constitutional right to due process." The court agreed, and dismissed the action without prejudice. This case is now on appeal to

the Ninth Circuit.

Winn-Dixie Stores (Florida): In June 2017, a Florida court issued an opinion finding that the Winn-Dixie website was subject to Title III as a service of a public accommodation (a grocery store), and must be accessible to the visually impaired.[12] The court's decision rested on whether the "website is heavily integrated with physical store locations and operates as a gateway to the physical location." The order cited cases where there was such an integration and cases where there is not. Ultimately the judge held that "the [Winn-Dixie] website is heavily integrated with Winn-Dixie's physical store locations and operates as a gateway to the physical store locations." For example, the Winn-Dixie website has coupons that can be used in stores, and consumers could refill prescriptions online and pick them up in stores. Because of this, he held that the site "heavily integrated" with the physical store locations and therefore is subject to the ADA.

For every public dispute, there are probably many more that take place in private. Over the past few years, plaintiffs' firms have been sending demand letters to companies alleging that their sites fail to comply with the ADA. Most demands or lawsuits settle quickly for less than it would cost to engage in meaningful litigation.[13] But as the number of firms sending these letters and filing these lawsuits has increased, an individual settlement may not buy the company much breathing room. Many companies are getting multiple demands, and least one court has held that a settlement agreement does not bar a later website accessibility brought by a different plaintiff.[14]

What to Do

If you are new to this area, you may wonder what website modifications may be necessary. Although the DOJ has not issued any regulations, most settlements in this area — including those involving the DOJ — require companies to comply with the Website Content Accessibility Guidelines 2.0 Level AA ("WCAG 2.0 AA"), published by the Web Content Accessibility Initiative of the World Wide Web Consortium ("W3C"). In absence of more specific guidance, compliance with the WCAG 2.0 AA guidelines is probably the closest a company can get to a "safe harbor."

If you don't know whether your website is accessible, now is the time to find out. Getting a sense of whether your site can be navigated by the use of a screen reader will give you a sense of whether your site could be considered a "low hanging fruit" for plaintiffs to target. You may not be able to get everything done overnight, but every step in the right direction can help.

Endnotes

1. 42 U.S.C. § 12182.
2. *See* 42 U.S.C. § 12181(7).
3. *Nat'l Fed'n of the Blind v. Target Corp.*, 452 F. Supp. 2d 946, 952 (N.D. Cal. 2006).
4. *Id.* at 955.
5. *National Federation of the Blind v. Scribd, Inc.*, 97 F.Supp.3d 565, 571 (D. Vt. Mar. 19, 2015).
6. *See e.g.*, *Cullen v. Netflix, Inc.*, 600 F. App'x 508, 509 (9th Cir. 2015) (Netflix not subject to ADA because Netflix's services not connected to any physical place); *Young v. Facebook, Inc.*, 790 F. Supp. 2d 1110 (N.D. Cal. 2011) (ADA claim fails because Facebook's internet services do not have a nexus to a physical place of public accommodation); *Earll v. eBay, Inc.*, No. 5:11-cv-00262-JF (HRL), 2011 U.S. Dist. LEXIS 100360 (N.D. Cal. Sept. 6, 2011).
7. *See e.g.*, Complaint, *West et al. v. Jo-Ann Stores LLC*, No. 1:16-cv-09386 (S.D.N.Y., Dec. 5, 2016).
8. *See e.g.*, Complaint, *Depina v. Houzz, Inc.*, Civ. No. 1:16-cv-12054 (D. Mass, Oct. 2016); Complaint, *Jahoda v. National Basketball Association*, No. 2:15-cv-1462 (W.D. Penn., Nov. 6, 2015).
9. *See* Complaint, *Farmer et al., SweetGreen, Inc.*, Civ. No. 1:16-cv-02103 (S.D.N.Y., Mar. 2016).
10. *Gomez v. Bang & Olufsen America, Inc.*, Case No.: 1:16-cv-23801 (S.D. Fla., Feb. 2, 2017) (Order Granting Defendant's Motion to Dismiss; Dismissing Plaintiff's ADA Claim Without Prejudice; and Administratively Closing the Case).
11. *Robles v. Domino's Pizza LLC*, Case No. 2:16-cv-06599 (C.D. Cal., Mar. 20, 2017) (Order Granting Defendant's Alternative Motion to Dismiss or Stay).
12. *Juan Carlos Gil v. Winn-Dixie Stores, Inc.*, Civil Action No. 16-23020-Civ-Scola (S.D. Fla. Jun. 13, 2017) (Verdict and Order Following Non-Jury Trial).
13. *See* Randazzo, S. (2016, Nov. 1) Companies Face Lawsuits Over Website Accessibility For Blind Users, *The Wall Street Journal*. Retrieved from http://www.wsj.com/articles/companies-face-lawsuits-over-website-accessibility-for-blind-users-1478005201 (last accessed Dec. 28, 2016).
14. *See Gniewskowski et al. v. Party City Holdings Co.*, Case No. 2:16-cv-01375-AJS (W.D. Pa., Jan 2017) (Memorandum Opinion).

The Long Arm of the European Privacy Regulator: Does the New EU GDPR Reach U.S. Media Companies?

KURT WIMMER

Since the advent of publishing on the Internet, media companies have been rightly concerned about the problem of international jurisdiction. Repeatedly, media companies with few contacts outside of the United States have been subjected to the jurisdiction of distant courts in countries from Australia to Zimbabwe applying their own domestic law to content that should be governed by the First Amendment and the standards set by U.S. law.[1]

One of the most significant concerns to media companies globally has been the rise of the so-called "right to be forgotten" in the European Union ("EU") and elsewhere, as well as the general ascendance of privacy concerns in the context of newsgathering and publishing news and information. The right to be forgotten, recently enforced against Google to require articles to be de-listed from search results, has a long history in the EU.[2] Two 2016 cases in Belgium[3] and Italy[4] required newspapers to anonymize articles under right to be forgotten petitions, with one saying that the public's right to information has an expiration date as short as two years. Although this trend has not been universal,[5] it is likely that publishers will continue to receive data anonymization orders from certain European courts.

This concept and a wide array of new privacy obligations are now part of the General Data Protection Regulation ("GDPR"), the largest and most significant overhaul of EU privacy law in more than 20 years. The GDPR will be a sea-change in EU privacy law for many reasons, including fines that can amount to as much as 4 percent of a company's *global* revenues and the creation of a new and powerful pan-European privacy regulatory agency.

The GDPR enters into force on May 25, 2018. European media companies, to be sure, are gearing up to comply with the GDPR. The open question for companies operating outside of the borders of Europe, however, is whether this stringent new regulation will apply to them, even though they have little or no actual presence within the EU.

The GDPR aspires to a broad jurisdictional reach, and is almost certainly intended to cover companies with websites that use cookies and other tracking devices to monitor people in the EU. Once subject to the GDPR's jurisdiction, a non-EU media company could be confronted with substantial enforcement burdens, such as court orders to fulfill right to be forgotten requests that would be untenable under American law — and face substantial fines for refusing to comply with such an order.

Even though the GDPR aspires to global jurisdiction, that aspiration does not answer the question of whether an EU law can have extraterritorial effect outside the boundaries of Europe. There are longstanding rules and norms of international jurisdiction that must be satisfied before regulatory agencies and courts can exercise jurisdiction over distant subjects.

This article analyzes those principles and concludes that pure U.S. media companies would have persuasive arguments against the jurisdiction of EU regulatory authorities and courts to enter orders against them, and a strong argument against the enforcement of such orders or subsequent fines. Aside from legal considerations, however, there may be significant reputational and practical issues that arise from resisting an order under the GDPR that companies will take into consideration.

I. The GDPR

The GDPR was developed with the goal of providing consistent privacy protections for individuals across the EU.[6] Prior to the adoption of the GDPR, each EU member country implemented its own data privacy laws under the guidance of the 1995 EU Data Protection Directive (the "Directive").[7] The result was a patchwork of somewhat divergent privacy protections among EU countries, which led to claims that companies could strategically select their EU country affiliations based on the strength of local privacy laws.[8] The GDPR aims to "harmoni[ze]" privacy laws in the EU by providing the same strong data protections for the entire region.[9]

In addition to harmonizing privacy protections across the board, the GDPR broadens the jurisdictional reach of the Directive.[10] The GDPR covers data controllers and processors outside the EU if they offer goods and services to, or monitor the behavior of, EU data subjects.[11] Behavior monitoring occurs when a natural person is "tracked on the internet," including the use of personal data to "profil[e] a natural person, particularly in order to take decisions concerning her or him or for analy[zing] or predicting her or his personal preferences, behavio[rs] and attitudes."[12] Personal data is defined as "any information relating to an identified or identifiable natural person 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as … [an] online identifier."[13] The intention behind this broad scope is to "ensure that individuals are not deprived of

Kurt Wimmer *U.S. Chair, Data Privacy and Cybersecurity Practice, Covington & Burling LLP, Washington, D.C..The author is grateful for the inspired assistance of Chloe Goodwin and Danielle Kehl, both members of the Class of 2018 at Harvard Law School.*

protection of their data" when they are in the EU, and to "enhance[] legal certainty for controllers and data subjects."[14] The GDPR's intended jurisdiction almost certainly aspires to cover websites and services outside of the EU that use cookies to monitor the behavior of individuals in the EU.

II. The Jurisdictional Aspirations of the GDPR

The GDPR contains a broad jurisdictional test. There are, however, specific principles under international law to assess when the extraterritorial reach of a state is permissible under international law.

A. Bases for International Jurisdiction

Under international law, there are several traditionally recognized bases for asserting jurisdiction, including the territoriality principle, the nationality principle, the passive personality principle, and the protective principle.[15] Especially with regard to online conduct, states have also increasingly exercised jurisdiction under variations of these principles such as the objective territoriality test and the effects doctrine.

Territoriality and Nationality. The most commonly invoked principles are territoriality and nationality, which permit states to assert jurisdiction over what happens within their borders[16] as well as over acts committed by individuals and organizations of the state's nationality (even if those acts take place outside of the state's physical territory).[17] A variation of the traditional territoriality concept is the so-called "objective territoriality principle," under which a state can assert jurisdiction over acts that were initiated abroad but completed within a state's territory, as well as where a "constitutive element of the conduct" occurred in the state.[18] The jurisdictional test in the Directive appears to be a manifestation of the objective territoriality principle because it allows European regulators to assert jurisdiction over foreign websites or online service providers based solely on their use of equipment or the location of servers within the EU.[19]

Passive Personality and the Protective Principle. In addition to asserting jurisdiction over acts committed abroad *by* their own nationals, states can sometimes assert jurisdiction for acts committed *against* their own nationals by foreigners. The passive personality principle permits states to exercise authority based on their connection to the victim of illegal conduct. Although this basis for jurisdiction has ordinarily been limited to serious crimes (*e.g.*, terrorist attacks or assassinations) as opposed to ordinary torts or crimes,[20] it has occasionally been applied in the civil law context as well.[21] The United States has traditionally disfavored exercising jurisdiction under this principle, but more recently U.S. courts have recognized it in certain instances such as acts of terrorism.[22] The protective principle extends this idea to allow the state to protect itself (rather than its citizens) from harmful acts inflicted outside of its territory.[23]

The Effects Doctrine. Finally, under the so-called "effects doctrine," states can assert jurisdiction based on the fact that conduct taking place entirely outside of the state has substantial effects within the state.[24] The concept is closely related to the objective territoriality idea, but it does not require that *any* element of the conduct being regulated actually take place within the territory of the state.[25] The effects doctrine is generally regarded as the most controversial basis upon which to assert jurisdiction under international law, but despite criticism from legal scholars has become widely used with regard to conduct over the internet.[26]

B. Reasonableness Analysis in International Jurisdiction

The mere fact that conduct or activity falls under one of these bases for jurisdiction does not necessarily justify its exercise. The current presumption in international law is that the party seeking to assert jurisdiction has to further prove why it is reasonable to exercise extraterritorial jurisdiction under any one of the bases described above.[27] The Third Restatement of Foreign Relations Law provides various factors for the courts to balance in making this determination — a limitation on the exercise of jurisdiction reflected in U.S. domestic law that has also emerged as a principle of international law.[28] These factors include:

(1) the link of the activity to the territory of the regulating state, including whether it has a "substantial, direct, and foreseeable effect,"

(2) the connections between the regulating state and the person who is principally responsible for the activity or the person who is supposed to be protected,

(3) the nature of the activity, its importance to the regulating state, and the extent to which other states regulate it,

(4) the "existence of justified expectations that might be protected or hurt by the regulation,"

(5) the importance of the regulation to the international system,

(6) the extent to which the regulation is consistent with the traditions of the international system,

(7) the extent to which another state may have an interest in regulating the activity, and

(8) the likelihood of conflict with regulation of another state.[29]

If an evaluation of these factors suggests that the extraterritorial application of the law in question would be unreasonable, courts are likely to find that there is no jurisdiction.

The concept of reasonableness described in the Third Restatement is also closely aligned with the principle of comity, which is often characterized as the "golden rule" among nations — that is, that each state should respect the laws, policies, and interests of other states just as it would have others respect its own in similar circumstances.[30] Comity dictates that states should generally

avoid extraterritorial application of their laws against foreign citizens where those laws conflict.[31] Where two states have concurrent jurisdiction over an individual or a particular act, states should do a balancing test and defer to the state whose interests are clearly greater.[32]

In data protection and other internet-related cases, determining whether a jurisdictional basis should be exercised can be quite complex. The courts may consider the place where the data controller is established; the place where personal data is stored or processed; the place where the allegedly wrongful act occurs; the residence of the data subject; and the use of cookies or similar technologies in another state.[33] If jurisdiction is based on the location of the data controller or the location where a marketing email is received, the exercise of that jurisdiction tends to be accepted under the territoriality principle and effects doctrine.[34] On the other hand, a more tenuous connection, such as the use of a single tracking cookie, might be viewed with greater skepticism even if it could be construed as falling under the effects doctrine or the protective principle.

Ultimately, the strongest grounds for a regulator to assert jurisdiction over a non-EU media company would be to base it on a combination of the objective territoriality principle, the passive personality principle, and the effects test.[35] There is a colorable argument that such an assertion of jurisdiction would nonetheless be unreasonable under the Third Restatement test or otherwise violate the principles of comity. A successful argument against the application of the GDPR would likely require showing that it conflicted with a U.S. law or regulation, such as the First Amendment's free speech and free press protections, and that the publisher's free expression interests outweigh the European Union's interest in safeguarding its citizens' privacy rights.

III. Enforceability of EU Orders

Even if European DPAs can properly assert jurisdiction over websites and online service providers under the GDPR's jurisdictional test, it is highly unlikely that a U.S. court would enforce an EU order requiring a newspaper to alter its contents under a right to be forgotten request, or a subsequent fine for not complying with such an order. This is largely due to the fact that any right to be forgotten order would very likely infringe upon the publisher's First Amendment rights.

A. The First Amendment and the Right to be Forgotten

Any right to be forgotten order directed at a newspaper would almost certainly violate the First Amendment. In general, freedom of press can only be restricted to "prevent grave and immediate danger to interests which the state may lawfully protect."[36] Further, the First Amendment protects the publication of "lawfully obtain[ed] truthful information about a matter of public significance . . . absent a need . . . of the highest order."[37]

Although the Supreme Court has acknowledged the significance of an individual's right to privacy, "privacy concerns give way when balanced against the interest in publishing matters of public importance."[38] A full analysis of this issue would depend on the facts of a particular case and is beyond the scope of this article, but given the primacy of the First Amendment it is unlikely that an order requiring a newspaper to alter its content or archived material would be construed as consistent with freedom of the press.[39]

B. Lack of Enforceability Under International Law

International law also distinguishes between the ability to *apply* versus *enforce* laws extraterritoriality. As such, even if the GDPR is applicable to certain conduct of U.S. companies under international law, penalties for violating the law may not actually be enforceable.[40] Much like the jurisdiction to prescribe, a state's ability under international law to exercise jurisdiction over a foreign individual through its courts is also limited by whether it is "reasonable."[41]

The two tests for reasonableness, however, are not the same. The reasonableness standard that countries must meet in order to assert jurisdiction to adjudicate focuses on whether the relationship between the state and the person over which it wishes to exercise jurisdiction is reasonable. The distinction between jurisdiction to prescribe and jurisdiction to adjudicate can be analogized to the difference between subject matter jurisdiction and personal jurisdiction in U.S. law.

Section 421 of the Third Restatement of Foreign Relations Law lays out the criteria for reasonableness in this area. Once again, a foreign company's permanent physical presence in the state would likely qualify as reasonable grounds to assert jurisdiction.[42] However, exercising jurisdiction over a company located entirely outside the EU whose only activity was the use of browser cookies to track individuals in the EU would likely be viewed with greater skepticism.[43] Although a European regulator could attempt to assert jurisdiction based on the effects of that monitoring within the state,[44] the publisher has a plausible argument that the use of cookies does not have a "substantial, direct, and foreseeable" effect and that it would therefore be unreasonable to assert jurisdiction on the basis of cookies alone.

C. Lack of Enforceability Under U.S. Common Law

Under the doctrine of comity, U.S. courts will generally grant extraterritorial effect to the valid judgments of foreign courts.[45] First, a U.S. court must be satisfied that the foreign court properly had jurisdiction over the matter at hand.[46] For reasons stated above, it is likely that a right to be forgotten order under the GDPR would fail to fulfill this requirement.

Even if a U.S. court finds that the foreign court did have jurisdiction over the case, comity does not extend to orders that are found to be contrary to public policy.[47] A foreign judg-

ment is considered contrary to public policy "to the extent that it is repugnant to fundamental notions of what is decent and just in the State where enforcement is sought."[48] Another formulation of this concept defines a foreign order as contrary to public policy when it "direct[ly] violat[es] the policy of our laws, and does violence to what we deem the rights of our citizens."[49] This is a very high standard that requires more than the mere fact that there are differences between foreign and domestic law.[50] Among the policy issues that are considered grounds for refusal to enforce foreign orders are those that implicate constitutional rights.[51]

When a foreign judgment is one that would violate the First Amendment, courts have found that it violates public policy and is thus unenforceable.[52] For example, courts have consistently refused to enforce UK orders related to libel, because English libel law is considered to be antithetical to First Amendment doctrine.[53] Because an order or fine under the GDPR related to the right to be forgotten would almost certainly violate the First Amendment, a U.S. court would likely refuse to enforce such an order from an EU court.

D. Lack of Enforceability Under U.S. Statutory Law: The SPEECH Act

There is an additional a statutory basis to argue that any penalties would be unenforceable under U.S. law. The Securing the Protection of Our Enduring and Established Constitutional Heritage (SPEECH) Act was enacted in 2010 to codify the common law presumption against enforcing foreign libel judgments in U.S. courts. Under the SPEECH Act, foreign libel judgments are unenforceable unless the legislation applied offers "at least as much protection for freedom of speech and press," or the defendant would have been found liable if the case had been heard under U.S. law.[54]

Although the SPEECH Act has rarely been invoked in the seven years since its passage, it could apply here either directly or by analogy. Interpreted broadly, the SPEECH Act suggests that all foreign judgments that would violate the First Amendment or chill free speech should be unenforceable through the U.S. court system if those cases are deliberately brought in jurisdictions whose laws are less protective of free speech — as would likely be the case with right to be forgotten actions brought against U.S. companies abroad.[55] And even if read narrowly to apply only to libel cases, the SPEECH Act and its legislative history[56] offer persuasive evidence that Congress certainly did not intend to foreign laws that violate the First Amendment to be enforced by U.S. courts.[57]

IV. Practical Consequences and Policy Considerations

As any general counsel knows, strict applicability of the law is only one factor in determining a company's potential responses to an enforcement action. Even if a publisher has a strong legal argument against being subject to the GDPR — and particularly right to be forgotten requests — there may be significant practical and reputational costs associated with defying Europe and European law.

Privacy is considered to be a fundamental right in the EU; freedom of press, on the other hand, does not enjoy the same reverence it receives in the United States.[58] In a public opinion poll on personal data processing, 89 percent of Europeans said it was important that their personal data should always receive the same level of protection, regardless of whether the company holding that data is established in the EU.[59] Publically resisting a new and significant EU privacy law may attach a negative stigma to a publisher in the minds of privacy-focused Europeans. Accordingly, public perception and policy considerations will surely play a significant role in media companies' calculus of how to approach compliance with EU privacy law generally, and the GDPR in particular.

In making this calculus, U.S. companies are likely to focus on their current and future approach to Europe. Elements of this calculus might include the importance of Europe as a market for advertising and home for subscribers, whether the company operates offices or bureaus in Europe and employs Europeans, and whether the company expects to expands its operations in the EU in the future. GDPR compliance requires a great deal more preparation than merely determining whether a company will comply with specific orders under sections of the GDPR dealing with the right to be forgotten or privacy rights relating to newsgathering, of course; any assessment of whether a company will comply with the GDPR will focus not only on the editorial side of any internet publisher but the business and ownership sides as well.

In making these multifaceted going-forward decisions, however, it may be useful to consider that the jurisdictional reach of the GDPR should be tempered by the application of longstanding international principles that govern jurisdiction. For a purely non-EU entity, a realistic view of the likely exercise and enforcement of jurisdiction would be a useful complement to a clear-eyed look at the business realities of working within Europe.

Endnotes

1. *See* Pogoriler, Satterfield and Wimmer, *International Jurisdiction and the Internet in an Age of Cloud Computing*, Bureau of National Affairs/ Bloomberg (2011); Wimmer, *Toward a World Rule of Law: Free Expression*, 603 *Annals of the American Academy of Political and Social Science* 202 (2006); Wimmer, *Enforcing Foreign Judgments in the United States and Europe: When Publishers Should Defend,* International Libel and Privacy Handbook: A Global Reference for Journalists, Publishers, Webmasters and Lawyers (C.J. Glasser, ed., Bloomberg Press, 2006).

2. *See, e.g.*, Case C-131/12, Google Spain v. Agencia Espanola de Proteccion de Datos, 2014 EUR-Lex CELEX 62012CJ0131 (May 13, 2014).

3 *See* Hugh Tomlinson, *"Right to*

be Forgotten" Requires Anonymisation of Online Newspaper Archive, University of London: Information Law and Policy Centre (July 26, 2016), https://infolawcentre.blogs.sas.ac.uk/2016/07/26/ right-to-be-forgotten-requires-anonymisation-of-online-newspaper-archive/#more-1162 (summarizing Cour de Cassation [Cass.] [Court of Cassation], Apr. 29, 2016, C.15.0052.F (Belg.)).

4. *See* Guido Scorza, *A Ruling by the Italian Supreme Court: News do Expire*, L'Espresso (July 1, 2016), http://espresso.repubblica.it/attualita/2016/07/01/news/a-ruling-by-the-italian-supreme-court-news-do-expire-online-archives-would-need-to-be-deleted-1.275720?ref=HEF_RULLO&refresh_ce (summarizing Cass., 24 giugno 2016, n. 13161/16 (It.)); Athalie Matthews, *How Italian Courts Used the Right to be Forgotten to Put an Expiry Date on News*, Guardian (Sept. 20, 2016), https://www.theguardian.com/media/2016/sep/20/how-italian-courts-used-the-right-to-be-forgotten-to-put-an-expiry-date-on-news.

5. *See* Kristof Van Quathem, *Right to be Forgotten: High Courts Disagree*, Inside Privacy (June 2, 2016), https://www.insideprivacy.com/international/european-union/right-to-be-forgotten-high-courts-disagree/ (summarizing Cour de Cassation [Cass.] [Court of Cassation], May 12, 2016, [15-17729](Fr.)); Emiel Jurjens, Google Spain in the Netherlands III, Media Report (June 5, 2015), http://www.mediareport.nl/en/press-law/05062015/google-spain-in-the-netherlands-iii-does-convicted-murderer-have-right-to-be-forgotten/ (summarizing Rechtbank Noord-Nederland, Groningen, 1 mei 2015, ([redacted]/Vereniging Voor Veiligheid, Respect en Soldariteit) (Neth.)).

6. *See* Council of the European Union, Draft Statement of the Council's Reasons 3 (Mar. 31, 2016) (providing the Council's reasons for proposing the GDPR and repealing the Directive) [hereinafter Council's Reasons]; The Greens/European Free Alliance, EU General Data Protection Regulation: State of Play and 10 Main Issues 1 (2015), http://www.janalbrecht.eu/fileadmin/material/Dokumente/Data_protection_state_of_play_10_points_010715.pdf [hereinafter State of Play].

7. *See* State of Play at 1; Christopher Kuner, *Data Protection Law and International Jurisdiction on the Internet (Part I)*, 18 Int'l J.L. & Info. Tech. 176, 179 - 80 (2010).

8. See State of Play at 1

9. Council's Reasons at 3.

10. *See, e.g.*, Allen & Overy, the EU General Data Protection Regulation 3 (2017).

11. Regulation 2016/679, art. 3(2), 2016 O.J. (L 119) 1, 32 - 33 [hereinafter GDPR].

12. *Id.* at 5.

13. *Id.*

14. Council's Reasons at 7.

15. *See* Restatement (Third) of Foreign Relations Law § 402 (Am. Law Inst. 1987) [hereinafter Rest. (Third)]. Although the Third Restatement primarily reflects the development of the law as it has been interpreted and enforced by U.S. courts, these rules (especially relating to the reasonableness of exercising extraterritorial jurisdiction) tend to be followed by other states and have emerged as principles of customary international law. *Id.* § 403 cmt. a.

16. *Id.* § 402(1)(a)-(b).

17. *Id.* § 402(2).

18. Kuner at 188.

19. *Id.*

20. Rest. (Third) § 402 cmt. g (noting that the passive personality principle "has not been generally accepted for ordinary torts or crimes, but it is increasingly accepted as applied to terrorist and other organized attacks on a state's nationals by reason of their nationality, or to assassination of a state's diplomatic representatives or other officials.").

21. Kuner at 188-89.

22. *See, e.g.*, United States v. Bin Laden, 92 F. Supp. 2d 189, 221 (S.D.N.Y. 2000) (upholding exercise of jurisdiction because while the U.S. has traditionally not exercised jurisdiction under the passive personality principle, it is increasingly accepted for acts of international terrorism).

23. Rest. (Third) § 402(3).

24. Rest. (Third) § 402(1)(c); Kuner at 190. *See also* Hartford Fire Ins. Co. v. California, 509 U.S. 764, 796 (1993) (holding that a domestic law "applies to foreign conduct that was meant to produce and did in fact produce some substantial effect in the United States.").

25. Int'l L. Comm'n, *Rep. on the Work of Its Fifty-Eighth Session*, U.N. Doc. A/61/10, at 521-22 (2006).

26. *Id.*

27. Rest. (Third) § 403(1).

28. *Id.* § 403 cmt. a.

29. *Id.* § 403(2)(a)-(h).

30. *See, e.g.*, Joel R. Paul, *Comity in International Law*, 32 Harv. Int'l L.J. 1, 11 (1991). Comity is "the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience." Hilton v. Guyot, 159 U.S. 113, 163-64 (1895).

31. *See, e.g.*, Hartford Fire Ins. v. California, 509 U.S. 764 (1993).

32. Rest. (Third) § 403 cmt. e.

33. Christopher Kuner, *Data Protection Law and International Jurisdiction on the Internet (Part 2)*, 18 Int'l J.L. & Info. Tech. 227, 237-40 (2010).

34. *Id.* at 241.

35. Cedric Ryngaert, *Symposium on Extraterritoriality and EU Data Protection*, 5 Int'l Data Privacy L. 221, 222 (2015).

36. W. Va. State Bd. of Educ. v. Barnette, 319 U.S. 624, 639 (1943).

37. Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 102 (1979).

38. Bartnicki v. Vopper, 532 U.S. 514, 533 (2001). It appears that the Supreme Court has yet to define what qualifies as a matter of public importance.

39. Many commentators have noted as much. *See, e.g.*, Eric Posner, *We all Have the Right to be Forgotten*, Slate (May 14, 2014, 4:37 PM), http://www.slate.com/articles/news_and_politics/view_from_chicago/2014/05/the_ european_right_to_be_forgotten_is_just_what_the_internet_needs.html; Robert

G. Larson III, *Forgetting the First Amendment*, 18 Comm. L. & Pol'y 91 (2013) (asserting the right to be forgotten is "fundamentally at odds with the right of freedom of speech").

40. Rest. (Third), ch. 4 (Introduction).

41. *Id.* § 421 cmt. a.

42. *Id.* § 421(2)(c). Permanent presence does not require actual residence in an EU member state, but "transitory presence" (*i.e.*, brief presence in a state enabling "tag" jurisdiction) would not satisfy the requirement. *Id.* § 421 cmt. e.

43. Kuner at 235.

44. Rest. (Third) § 421(j) states that an exercise of jurisdiction to adjudicate is reasonable if "the person… had carried on outside the state an activity having a substantial, direct, and foreseeable effect within the state, but only in respect of such activity."

45. *See* Ritchie v. McMullen, 159 U.S. 235, 243 (1895); Velsicol Chem. Corp. v. Hooker Chem. Corp., 230 F. Supp. 998, 1018 (N.D. Ill. 1964); Gull v. Constam, 105 F. Supp. 107, 108 (D. Colo. 1952).

46. *See* Ackermann v. Levine, 788 F.2d 830, 837 (2d Cir. 1986).

47. Corporacion Mexicana De Mantenimiento Integral v. Pemex-Exploracion Y Produccion, 832 F.3d 92, 96 (2d Cir. 2016); *see* Hilton v. Guyot, 159 U.S. 113, 193 (1895); Rest. (Second) of Conflict of Laws § 117 cmt. c.

48. *See Ackermann*, 788 F.2d at 841.

49. *See Hilton*, 159 U.S. at 193.

50. *See id.* at 194; Somportex Ltd. v. Pa. Chewing Gum Corp., 318 F. Supp. 161, 168 (E.D. Pa. 1970).

51. *See, e.g.*, Mata v. Am. Life Ins. Co., 771 F. Supp. 1375, 1384 (D. Del. 1991) (due process).

52. See Matusevitch v. Telnikoff, 877 F.Supp. 1, 2 (D.D.C. 1995) ("Because recognition and enforcement of a foreign judgment, based on libel standards that are repugnant to the public policies of the State of Maryland and the United States, would deprive the plaintiff of his First and Fourteenth Amendment rights, the court grants summary judgment for the plaintiff as a matter of law.").

53. *See id.*; Abdullah v. Sheridan Square Press, Inc., 1994 WL 419847, at *1 (S.D.N.Y. May 4, 1994) ("Since establishment of a claim under the British law of defamation would be antithetical to the First Amendment-protections accorded the defendants, the second cause of action alleged in the complaint is dismissed." (citation omitted)); Bachchan v. India Abroad Publ'ns Inc., 585 N.Y.S.2d 661, 662 (Sup. Ct. 1992) (denying summary judgment on the grounds that "[t]he protection to free speech and the press embodied in [the First Amendment] would be seriously jeopardized by the entry of foreign libel judgments granted pursuant to standards deemed appropriate in England but considered antithetical to the protections afforded the press by the U.S. Constitution").

54. 28 U.S.C. §§ 4101-05.

55. In the findings section of the bill, Congress noted that "[t]he freedom of speech and the press is enshrined in the first amendment to the Constitution, and is necessary to promote the vigorous dialogue necessary to shape public policy in a representative democracy" and that "[s]ome persons are obstructing the free expression rights of United States authors and publishers, and in turn chilling the first Amendment to the Constitution of the United States interest of the citizenry in receiving information on matters of importance, by seeking out foreign jurisdictions that do not provide the full extent of free-speech protections. . . that are available in the United States."

56. *See, e.g.*, S. Rept. 111-224, at 8 (2010) (noting that "[t]he SPEECH Act will ensure that no domestic court can be used to diminish the First Amendment rights of American authors, reporters and publishers by enforcing a foreign libel judgment that is inconsistent with U.S. law. . . . This bill will prevent the chilling of American free speech that is the inevitable result of these foreign libel lawsuits.").

57. Dana Green, *The Speech Act Provides Protection Against Foreign Libel Judgments*, Am. Bar Ass'n (n.d.), http://apps.americanbar.org/litigation/litigationnews/mobile/firstamendment-SPEECH.html (noting that "[t]he act's symbolic significance, as an expression of the depth of Congressional commitment to free speech, should be heartening to free speech advocates").

58. *See generally* Adam Liptak, *When American and European Ideas of Privacy Collide*, N.Y. Times (Feb. 27, 2010), http://www.nytimes.com/2010/02/28/weekinreview/28liptak.html.

59. Vera Jourova, Data Protection: Factsheet 4 (2015), http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf.

Court Ends Its Term With Two Broad First Amendment Rulings

Jessica Ring Amunson and Imara H. McMillan

As the Supreme Court's 2016 Term drew to a close, the Court reaffirmed core First Amendment principles in two opinions—*Matal v. Tam* (formerly *Lee v. Tam*) and *Packingham v. North Carolina*—both issued on June 19th. In *Matal*, the Court held that the anti-disparagement provision of the Lanham Act amounted to unconstitutional viewpoint discrimination under the First Amendment. In *Packingham*, the Court struck down a North Carolina statute prohibiting registered sex offenders from accessing websites where minors are known to be active, regardless of whether the sex offender directly contacted a minor, as overbroad in violation of the First Amendment. Although both cases were decided unanimously, each left some important questions unanswered.

In *Matal,* musician and social activist Simon Tam attempted to trademark the name of his all-Asian American band, "The Slants." The U.S. Patent and Trademark Office ("PTO") denied the application under Section 2(a) of the Lanham Act, which prohibits trademarks that "consist[] of or comprise[] 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."[1] The PTO found the name would likely be disparaging towards persons of Asian descent. Tam was well aware of this. In fact, he chose the name of his band in 2006 precisely *because* it was disparaging. He hoped to reclaim a slur that had been used to insult members of the Asian-American community for years. Tam appealed the PTO's decision, and while the Federal Circuit initially upheld the PTO, the court then *sua sponte* ordered *en banc* rehearing, and found that the anti-disparagement provision of Section 2(a) violates the First Amendment.

The Supreme Court agreed with the *en banc* Federal Circuit about the statute's unconstitutionality. The Court found that Section 2(a) violated a bedrock First Amendment principle: "the government may not prohibit the expression of an idea simply because society finds the idea itself offensive or disagreeable."[2] The entirety of the Court agreed that the Section 2(a) violated the Free Speech Clause and there was also unanimous agreement that trademarks are not government speech. The Court divided, however, on its rationale as to the remainder of the government's arguments. In an opinion written by Justice Alito and joined by Chief Justice Roberts, Justice Thomas, and Justice Breyer, the Court concluded that trademarks were neither government provided subsidies nor government programs; two other areas where the Court has occasionally determined viewpoint discrimination is constitutional. Additionally, Justice Alito's opinion found that Section 2(a) was not a permissible regulation of commercial speech because it was not narrowly drawn to serve a substantial interest, under the relaxed scrutiny afforded by *Central Hudson* review. As Justice Alito wrote: The clause "is not an anti-discrimination clause; it is a happy-talk clause. In this way, it goes much further than is necessary to serve the interest asserted."[3]

Justice Kennedy, joined by Justices Ginsburg, Sotomayor, and Kagan, wrote a concurring opinion expounding on the fact that Section 2(a) constitutes viewpoint discrimination. Jus- , "To permit viewpoint discrimination in this context is to permit Government censorship."[4] His opinion also pointed out that the majority opinion did not address how other provisions of the Lanham Act should be interpreted under the First Amendment. Thus, while First Amendment scholars will appreciate the clarity of the Court's opinion, trademark lawyers may find *Matal* less than satisfying for the Lanham Act questions it leaves unresolved.

The Court also left some unanswered questions in *Packingham*. In 2010, Lester Packingham, a registered sex offender, was arrested after authorities found a post on his Facebook profile thanking God for the dismissal of a traffic ticket. North Carolina law makes it a felony for a registered sex offender to "access a commercial social networking website where the sex offender knows that the site permits minor children to become members or to create or maintain personal web pages."[5] Packingham argued that the law violated his First Amendment rights, but was convicted in trial court. However, the North Carolina Court of Appeals reversed his conviction and held that social media website provision of the law was unconstitutional. The North Carolina Supreme Court found that the law was a limitation on conduct, rather than a restriction of free speech, and reinstated the conviction. Packingham sought review in the Supreme Court.

While the Court unanimously agreed that the North Carolina law was unconstitutional, the justices were split as to the breadth of the holding. Justice Kennedy's majority opinion acknowledged that the State has a legitimate interest in protecting children from abuse. However, he noted that "it is well established that, as a general rule, the Government may not suppress lawful speech as the

Jessica Ring Amunson *is the co-chair of the Appellate & Supreme Court Practice at Jenner & Block LLP, and* **Imara H. McMillan** *is a Sponsors for Educational Opportunity Fellow at Jenner.*

means to suppress unlawful speech."[6] The Court found that North Carolina's law did just that and was overly broad. Under its provisions, the law might well bar access to not only to Facebook and other social media websites, but also to Amazon, The Washington Post, and WebMD. The Court found that the State's law was not necessary, or legitimate, to serve the purpose of keeping sex offenders away from vulnerable potential victims.

Justice Alito, joined by Chief Justice Roberts and Justice Thomas, wrote a concurring opinion that attempted to set boundaries on what they characterized as the majority opinion's "undisciplined dicta."[7] Justice Alito took issue with Justice Kennedy for equating the entirety of the internet with public streets and parks. In Justice Alito's view, "Cyberspace is different from the physical world, and if it is true, as the Court believes, that 'we cannot appreciate yet' the 'full dimensions and vast potential of the Cyber Age,' we should proceed circumspectly, taking one step at a time. It is regrettable that the Court has not heeded its own admonition of caution."[8]

Thus, while both opinions unanimously reaffirmed several basic First Amendment tenets, there are important divisions among the Court as to the application of these tenets that First Amendment scholars and practitioners will be closely watching.

Endnotes

1. 15 U.S.C. § 1052(a).
2. *Matal v. Tam*, 582 U. S. ____ (2017), slip op. at 23.
3. *Id.* at 25.
4. *Id.* at 6 (Kennedy, J., concurring)
5. N.C. Gen. Stat. Ann. §§14–202.5(a), (e).
6. *Packingham v. North Carolina*, 582 U.S. ____ (2017), slip op. at 10.
7. *Id.* at 1 (Alito, J., concurring)
8. *Id*. at 11.

Prosecution of Journalists Under the Espionage Act? Not So Fast.

Kurt Wimmer and Stephen Kiehl

No journalist has ever been prosecuted under the Espionage Act. There long has been debate over whether the statute could apply to journalists, however, and there is newfound concern that the Trump Administration—led by a president who has openly declared "war with the media"[1]—will pioneer such a prosecution. The recent prosecution of NSA contractor Reality Winner for leaking sensitive information to the *Intercept* indicates that the Trump Administration will not hesitate to use the Espionage Act to pursue leakers,[2] a practice that was employed by the Obama Administration.[3]

Although administrations have generally interpreted the Espionage Act so as not to apply to journalists,[4] either through the "mercy of *noblesse oblige*"[5] or prosecutorial self-restraint, Attorney General Jeff Sessions refused to commit to upholding this tradition when asked about it at his confirmation hearings.[6] And, as a senator and the Republican leader on the Senate Judiciary Committee, Attorney General Sessions consistently opposed proposals to create a federal privilege to permit journalists to protect the identity of sources, decrying the laws as means of "protect[ing] those who use the media to illegally expose America's national security secrets."[7]

Some writers recently have focused on the language of the Espionage Act and, based on nothing more, asserted that journalists certainly could be prosecuted under that Act. But reading the text of a statute, of course, is only the first step in determining whether a criminal law could be used to silence or punish the press. Quite to the contrary, we see a number of defenses and bases on which prosecution of journalists under the Espionage Act would be improper and even unconstitutional.

First, a proper construction of Section 793(e) would avoid the overwhelming constitutional issues and find that the statute does not, and was not meant to, apply to journalists engaged in the act of publishing and reporting. *Second*, if Section 793(e) is held to apply to journalists on its face, then the statute, as applied to journalists publishing information in the course of their profession, violates the First Amendment and any prosecution under it would be invalid. The statute constitutes a content-based restriction, subject to strict scrutiny, and the government cannot overcome its burden of proving that the prosecution of journalists is narrowly tailored to protect national security. *Third,* there are several additional ways in which the prosecution of a reporter would be unconstitutional: the statute is unconstitutionally vague; this rare application of the statute constitutes selective prosecution; and the statute amounts to a prior restraint.

The Text of the Espionage Act

The Espionage Act was first passed by Congress in 1917, after America entered World War I, and amended through the Internal Security Act of 1950. Now codified at 18 U.S.C. §§ 793-798, the part that poses the greatest and broadest risk to journalists is Section 793(e).

Section 793(e) provides for the fine or imprisonment of:

> Whoever having unauthorized possession of, access to, or control over any document, writing[,] or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted … the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it.[8]

At the outset, it is worth emphasizing that Section 793(e) is limited to documents and information "relating to the national defense." This is a term of art that would not encompass every leak coming out of the government, or all classified information. Rather, to qualify as information "relating to the national defense," the information must be (1) "potentially damaging to the United States or might be useful to an enemy of the United States," and (2) "closely held" by the government.[9]

With that caveat in mind, the statute's text would seem to apply to a journalist who has obtained leaked information that is related to the national defense. She possesses information that she is presumably unauthorized to possess, and the information pertains to the "national defense."[10] If the information was considered to be a "document," "writing," or "note," she would violate the statute by willfully continuing to possess the document without turning it in (not to mention willfully "communicat[ing]" or "transmit[ing]" it).[11]

If the journalist possessed only "information"—i.e. not a physical piece of U.S. property—she would need to have "reason to believe" the information could be used to "injur[e]" the United States or help "any foreign nation."[12] Though "reason to believe" is a higher *mens rea* requirement than "willfulness," it does not provide much comfort as many notable leaks—such as the news that President Trump shared national security intelligence with the Russian foreign minister—would give the author "reason to believe" that the information could adversely affect the United States and aid foreign nations. In other words, as Harold Edgar and Benno C. Schmidt said in their pivotal

Kurt Wimmer and Stephen Kiehl *Covington & Burling LLP, Washington, D.C.* *The authors are grateful for the inspired research and analysis of Samson Schatz, Stanford Law Class of 2018, without whom this article would not be possible.*

1973 piece on the Espionage Act, "If these statutes mean what they seem to say and are constitutional, public speech in this country since World War II has been rife with criminality."[13]

The Proper Interpretation of the Act, Consistent with the Constitution

1. Section 793(e) Does Not Apply to Journalists Engaged in theAct of Reporting and Publishing.

A foundational defense is that Section 793(e), when considered in its statutory context and with its legislative history, does not apply to journalists exercising their First Amendment rights. The statute can—and should—be construed to avoid a conflict with the First Amendment. The Supreme Court has allowed that courts may "strain to construe legislation so as to save it against constitutional attack" though they "must not and will not carry this to the point of perverting the purpose of a statute."[14] Because the Espionage Act is highly politicized, confusing, and old, courts have significant incentive to avoid constitutionalizing the issues and to simply read Section 793(e) so as not to apply to journalists acting in the course of their profession. This is not nearly as implausible as some have assumed.

First, Section 793(e) forbids "communicat[ion], deliver[y], or transmiss[ion]" but does not specifically include "publication."[15] Though it may seem trivial to argue that the act of publishing does not lie within the plain meaning of communication, delivery, or transmission,[16] Congress arguably understood the act of publishing as separate and unique from the other actions. In Sections 794, 797, and 798, Congress specifically forbids the act of "publishing" certain information, at certain times.[17] If the words in § 793(e)—"communicates, delivers, [or] transmits"—included "publishing," the subsequent statutes would be redundant. Justices Douglas and Black, concurring in the judgment in *New York Times Co. v. United States*,[18] understood the omission of *publishing* from Section 793(e) to mean that the statute "does not apply to the press."[19] The Supreme Court has emphasized that "where Congress includes particular language in one section of a statute but omits it another … it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion of exclusion."[20]

Second, a reading of "willful"—"willfully communicates, delivers, [or] transmits" and "willfully retains"[21]—precludes journalists acting in the course of their business. Edgar and Schmidt read Section 793(e) such that "conduct is not willful for purposes of the Section, when undertaken for any of the variety of reasons . . . that reflect interests protected by the First Amendment."[22] In other words, when acting in the course of their business—reporting, writing, and publishing news, all actions that are critical to the foundational freedom of the press—journalists *cannot* satisfy the *mens rea* elements contained in the statute.

The legislative histories of the 1917 and 1950 acts—as interpreted by Edgar and Schmidt in their exhaustive study of these statutes—convey a "clear message" that "publication of defense information for the purpose of selling newspapers or engaging in public debate is not a criminal act."[23] Edgar and Schmidt walk carefully through the record of Congressional speeches and letters to show that these acts were not understood by their authors to criminalize the work of reporters.[24] Judge Gurfein—the judge presiding over the *Pentagon Papers* case at the district court—also found the legislative history persuasive.[25] Judge Gurfein quotes Senator Ashhurst's statements during congressional debate over the 1917 Act: "'[F]reedom of the press' means nothing except that the citizen is guaranteed that he may publish whatever he sees fit and not be subjected to pains and penalties because he did not consult the censor before doing so."[26] These words informed Judge Gurfein's confidence that Congress did not intend for the Act to apply to journalists in the course of their work.

And perhaps the best illustration of congressional intent is the opening proviso to the Internal Security Act of 1950 (the act that amended Section 793(e) to its current form): "Nothing in this Act shall be construed to authorize, require, or establish military or civilian censorship or in any way to limit or infringe upon freedom of the press or of speech as guaranteed by the Constitution of the United States and no regulation shall be promulgated hereunder having that effect."[27] These are powerful words that should give any court confidence to narrowly construe Section 793(e) so as not to apply to journalists.

2. The Espionage Act Is an Unconstitutional Content-Based Restriction of Freedom of the Press.

To the extent Section 793(e) is applied to journalists, it clearly restricts First Amendment activity in proscribing what journalists may or may not publish ostensibly in the name of national security. The First Amendment provides that "Congress shall make no law . . . abridging the freedom of speech, or of the press."[28] "The predominant purpose of the [First Amendment] . . . was to preserve an untrammeled press as a vital source of public information. . . .[S]ince informed public opinion is the most potent of all restraints upon misgovernment, the suppression or abridgment of the publicity afforded by a free press cannot be regarded otherwise than with grave concern."[29] In fact, "[t]he press was protected so that it could *bare the secrets of government* and inform the people. Only a free and unrestrained press can effectively expose deception in government."[30]

With this grave concern for preserving the vital role of the press in our democratic system, courts approach restraints of the press with a high degree of skepticism. Therefore, if Section 793(e) is deemed to apply to journalists on its face, then as applied, the statute constitutes a content-based restriction. And "[c]ontent-based laws—those that target speech based on its communicative content—are presumptively unconstitutional and may be justified only if the government proves that they are narrowly tailored to serve compelling state interests."[31]

A regulation is content-based if the "law applies to particular speech because of the topic discussed or the

idea or message expressed."[32] In *Reed v. Town of Gilbert*, the Supreme Court affirmed that if a law is content-based on its face, a court need not inquire as to the legislature's purposes for enacting the statute in order to apply strict scrutiny.[33] Section 793(e), on its face, constitutes a content-based restriction on speech. The statute only restrains speech pertaining to the national defense.[34]

Under strict scrutiny, the court asks whether the statute is narrowly drawn to serve the government's compelling interests. Here, there is no dispute that preserving the national defense is a compelling interest.[35] Therefore, the analysis turns to whether prosecuting journalists under Section 793(e) is necessary to protect that interest.

Prosecuting journalists under Section 793(e) is not narrowly tailored to safeguard America's national security for three reasons: (1) prosecuting journalists is an ineffective way to achieve the government's compelling interests; (2) the law is overinclusive; and (3) there are less restrictive alternatives to safeguarding national security without causing such damage to First Amendment freedoms.

First, the law does not actually protect national security—at least not in a constitutional way. The government has the burden of proving the "harms it recites are real and that its restriction will in fact alleviate them to a material degree."[36] Therefore, the law fails narrow tailoring if it does not effectively promote the government's stated interests. Here, prosecuting journalists under Section 793(e) does not make anyone safer.

In fact, the government may be caught in a logical bind: The government will argue that this law does not constitute a prior restraint on speech in that it only punishes publication after the fact. But if we accept the government's argument there as true, how does the law actually protect national security? The logical answer is that it provides deterrence—by criminally prosecuting journalists for publishing sensitive information, future journalists will think twice about doing the same. This explanation, however, brings the government right back into the highly scrutinized area of prior restraint. By arguing that deterrence is what makes the law effective, the government tacitly admits the statute functions as a prior restraint. Thus, Section 793(e) is either ineffective and thus unconstitutionally applied to journalists for lack of narrow tailoring, or it *is* effective and thus an unconstitutional prior restraint.

Second, the law is overinclusive. On its face, the law brings under threat of criminal liability a tremendous amount of newsworthy reporting that does not threaten national security (or at least where the risks to national security are far outweighed by the public interest). Several examples highlight the dangerous reach of the law:

- On January 12, 2017, the Washington Post reported that Retired Lt. Gen. Michael T. Flynn, the incoming national security advisor, had spoken on the phone with Russian Ambassador, Sergey Kislyak several times, after telling Vice President-elect Pence and others that he had not.[37] Presumably, Post columnist David Ignatius had "unauthorized possession" of this information which might be broadly interpreted as pertaining to the national defense, and had reason to believe that revealing the information could be used to embarrass or otherwise harm the United States. Ignatius would therefore be liable for criminal prosecution under Section 793(e), even though the public interest in reporting this news far outweighs any concerns about protecting the national defense.

- In May 2017, the Washington Post reported that President Trump revealed highly classified information—shared with the United States by a close ally—to the Russian foreign minister and ambassador.[38] Again, if Section 793(e) applied to journalists, its elements may be met here and the journalists could be criminally liable, even though the information is a matter of critical public interest.

These example highlight the nature of the public interest that is at stake if the Espionage Act is deemed applicable to journalists. Either these journalists must jeopardize their own liberty to report newsworthy facts, or very possibly, the facts never make their way into the public sphere. The First Amendment saves journalists from deciding between those two choices.

Lastly, Section 793(e) is not narrow tailored because there are numerous alternatives through which the government can safeguard national security without so severely burdening First Amendment rights.[39] One alternative is for the government to continue its informal negotiations with media organizations when a specific issue of concern arises. A common practice among the press, already, is to approach the government with a piece of leaked information before publishing stories about it.[40] Second, journalists can still be prosecuted or sued under generally applicable criminal and civil laws.[41] The government can use applicable criminal laws to guarantee that journalists do not steal sensitive information or otherwise coerce sources to break the law. A third alternative is to prosecute government employees who leak information, rather than journalists who publish the information, as the Obama and now Trump administrations have done. Courts have generally held that there are no First Amendment rights implicated in the prosecution of government employees who have breached the terms of their employment by leaking classified materials.[42]

3. Section 793(e) Is Unconstitutionally Vague.

The century of speculation and confusion over whether the text of the Espionage Act can be applied to journalists is a testament to its vagueness. "A conviction fails to comport with due process if the statute under which it is obtained fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement."[43] And in the context of the First Amendment, courts are particularly vigilant about statutory vagueness given the immense concern over chilling speech.[44]

Simply put, no one understands

what the Espionage Act really means or how it should be applied, particularly with respect to journalists, and its vagueness affords the government "too much enforcement discretion."[45] For example, how should "unauthorized possession" be defined?[46] Does this imply tethering to the government's classification system, wherein only classified materials can be possessed without authority and only by persons who do not have clearances?[47] Must something be affirmatively determined "unauthorized" or, conversely, is anything that is *not* specifically unauthorized, authorized? Perhaps in the context of the 1950 Internal Security Act proviso, the First Amendment freedom of the press suffices to convey "authority"?

Furthermore, as discussed above, is publishing considered "communicating, delivering, or transmitting"? And, what constitutes "willful[] ret[ention]" of "information" when it is not one of the enumerated physical items pertaining to the national defense?[48] What must a journalist do to avoid criminal liability if she is told a sensitive piece of information over the phone? These glaring ambiguities fall far short of giving a person of average intelligence fair notice of what is and is not criminal under the statute.[49] After all, if they are "beyond [the] ken" of former FBI director and career prosecutor James Comey,[50] who can possibly be expected to be on notice?

4. Unconstitutional Selective Prosecution.

Due to the non-existence of journalist prosecutions under Section 793(e), a journalist charged under the section today would have a persuasive selective prosecution claim. Generally the government retains "broad discretion" in its decisions of who to prosecute and when.[51] The Supreme Court has recognized that this discretion, however, is subject to ordinary equal protection standards, which require "petitioner to show both that the [decision to prosecute] had a discriminatory effect and that it was motivated by a discriminatory purpose."[52] In *Wayte v. United States*, petitioners were prosecuted for failure to register for the draft.[53] The only non-registrants prosecuted, however, were those who affirmatively protested the draft and notified the government of their intention not to register. Those who remained silent were not prosecuted.[54] Petitioners argued they were prosecuted in retaliation for the exercise of their First Amendment rights.[55] The government responded that it was simply prosecuting individuals who had identified themselves as violating the law—it was purely a passive enforcement system.[56] The Court sided with the government, holding that petitioners failed to show that the government was discriminating against non-registrants on the basis of their speech.[57]

A journalist's claim of selective prosecution in retaliation for exercising her First Amendment rights is more likely to succeed than the non-registrants' claims in *Wayte*. That said, the success of her claim may rise or fall on the existence of several additional facts. For example, she would have a stronger discriminatory effects claim if she can show that most journalists are not prosecuted for publishing leaked information, but only she and others who are particularly critical of the administration suffer prosecution. In addition, she may succeed in claiming discriminatory intent if she can show, for example, that the administration or other policy makers sometimes strategically leak their own information to the press, and when they do so, the journalists publishing that information remain safe from prosecution,[58] whereas when journalists who do not receive such information from the administration publish stories containing leaks, *they* are prosecuted.

These facts are not preposterous. Former L.A. Times Editor Dean Baquet and former New York Times Editor Bill Keller describe a situation in which former Treasury Secretary John Snow invited a group of reporters to tour the department's capabilities for tracking terrorist financing for several days. Throughout the trip, the secretary's team shared many sensitive details of their efforts and capabilities, hoping they would appear in print.[59] Three years later, Secretary Snow vehemently protested the papers' decision

andled bank-monitoring program. "Government officials, understandably, want it both ways."[60] Yet, such hypocrisy, while understandable, can be potent evidence of discriminatory purpose if the government decides to start prosecuting certain journalists.

5. The Espionage Act Amounts to a Prior Restraint.

This is not a typical prior restraint. Traditionally the Supreme Court has drawn a distinction between "criminal or civil sanctions after publication" and prior restraints.[61] Both can be violative of the First Amendment—the former "chills" speech, the latter "freezes" it[62]—but prior restraints are especially disfavored.[63]

In one case, however, the Supreme Court entertained, without deciding, a party's argument that a criminal statute acts in "operation and effect" like a licensing scheme and thus constituted a prior restraint.[64] As applied to journalists, Section 793(e) may also be an atypical criminal statute that amounts to a prior restraint given its singular purpose of deterring journalists from publishing sensitive information pertaining to the national defense. As briefly noted above, it is hard to read the statute as achieving its purpose of protecting national security in any other way but to effectively restrain journalists from publishing stories. In that case, Section 793(e) acts in "operation and effect" like a prior restraint, and should bear a "heavy presumption against its constitutional validity."[65]

Conclusion

If this Administration, or any future one, chooses to test the boundaries of the Espionage Act by prosecuting a journalist for the publication of sensitive information, defenders of the press will have multiple paths to showing that such a prosecution is improper. A court may employ basic tenets of statutory interpretation to find that Section 793(e) on its face does not apply to "publishing" information, thus avoiding a constitutional confrontation. If a court reads the Espionage Act to apply to journalists, it will be forced to grapple with compelling constitutional arguments that the act is not narrowly

tailored to achieve its purpose and is unconstitutionally vague, and that its use amounts to a selective prosecution or prior restraint. For good reason, the Supreme Court has repeatedly reaffirmed that "'state action to punish the publication of truthful information seldom can satisfy constitutional standards.'"[66]

Endnotes

1. Julian Zelizer, *President Trump's Dangerous War on the Media*, CNN (Jan. 25, 2017), http://www.cnn.com/2017/01/25/opinions/trumps-war-on-media-zelizer-opinion ("I have a running war with the media. They are among the most dishonest human beings on earth, right?").

2. Charlie Savage et al., *Reality Winner, N.S.A. Contractor Accused of Leak, Was Undone by Trail of Clues*, N.Y. Times (June 6, 2017), https://www.nytimes.com/2017/06/06/us/politics/reality-leigh-winner-leak-nsa.html.

3. *See* James Risen, *If Donald Trump Targets Journalists, Thank Obama*, N.Y. Times (Dec. 30, 2016), https://www.nytimes.com/2016/12/30/opinion/sunday/if-donald-trump-targets-journalists-thank-obama.html?_r=0.

4. *See, e.g.*, Zachary Roth, *Holder: I Won't Send Journalists to Jail for Doing Their Job*, MSNBC (Oct. 14, 2014), http://www.msnbc.com/msnbc/holder-i-wont-send-journalists-jail-doing-their-job ("no reporter is going to go to jail as long as I am attorney general").

5. United States v. Stevens, 559 U.S. 460, 480 (2010) ("We would not uphold an unconstitutional statute merely because the Government promised to use it responsibly.").

6. Peter Sterne, *Sessions 'Not Sure' Whether He Would Prosecute Journalists*, POLITICO (Jan. 10, 2017), http://www.politico.com/blogs/on-media/2017/01/sessions-not-sure-whether-he-would-prosecute-journalists-233431 (quoting Sessions as saying that "you could have a situation in which media's not the unbiased media we seen [sic] today, and they could be a mechanism through which unlawful intelligence is obtained").

7. *A Report on Attorney General Nominee Jeff Sessions on Issues that Affect the News Media*, Reporters Comm. for Freedom of the Press, https://www.rcfp.org/sessions-report (last visited June 22, 2017).

8. 18 U.S.C. § 793(e) (2015)

9. United States v. Morison, 844 U.S. 1057, 1071-72 (4th Cir. 1988) (citation omitted).

10. *Id.*

11. *Id.*

12. *Id.*

13. Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 Colum. L. Rev. 929, 1000 (1973).

14. Holder v. Humanitarian Law Project, 561 U.S. 1, 17 (2010) (quoting Scales v. United States, 367 U.S. 203, 211 (1961)).

15. 18 U.S.C. § 793(e) (2015).

16. *See* Edgar & Schmidt, *supra* note 13, at 1036.

17. 18 U.S.C. §§ 794, 797, 798 (2015).

18. 403 U.S. 713 (1971).

19. *Id.* at 721 (Douglas, J., concurring).

20. Keene Corp. v. United States, 508 U.S. 200, 208 (1993) (citation omitted).

21. 18 U.S.C. § 793(e) (2015).

22. Edgar & Schmidt, *supra* note 13, at 1046.

23. *Id.* at 1001-02.

24. *See id.* at 1002-31

25. *See* United States v. New York Times Co., 328 F. Supp. 324, 329 (S.D.N.Y. 1971).

26. *Id.*

27. Internal Security Act of 1950, H.R. 9490, 81st Cong. § 1(b), 64 Stat. 987 (1950).

28. U.S. Const. amend. I.

29. Grosjean v. Am. Press Co., 297 U.S. 233, 250 (1936).

30. New York Times Co. v. United States, 403 U.S. 713, 717 (1971) (Black, J., concurring) (emphasis added).

31. Reed v. Town of Gilbert, 135 S. Ct. 2218, 2226 (2015).

32. *Id*. at 2227.

33. *Id.*

34. *See* 18 U.S.C. § 793(e) (2015)

35. *See, e.g.*, *Humanitarian Law Project*, 561 U.S. at 34-36; *see also id.* at 28 ("Everyone agrees that the Government's interest in combating terrorism is an urgent objective of the highest order.")

36. Edenfield v. Fane, 507 U.S. 761, 770–71 (1993)

37. David Ignatius, *Why did Obama Dawdle on Russia's Hacking?* Wash. Post (Jan. 12, 2017), https://www.washingtonpost.com/opinions/why-did-obama-dawdle-on-russias-hacking/2017/01/12/75f878a0-d90c-11e6-9a36-1d296534b31e_story.html?utm_term=.dc7f8d4b5214.

38. Greg Miller & Greg Jaffe, *Trump Revealed Highly Classified Information to Russian Foreign Minister and Ambassador*, Wash. Post (May 15, 2017), https://www.washingtonpost.com/world/national-security/trump-revealed-highly-classified-information-to-russian-foreign-minister-and-ambassador/2017/05/15/530c172a-3960-11e7-9e48-c4f199710b69_story.html?utm_term=.75804b29efc5.

39. *See, e.g.*, McCullen v. Coakley, 134 S. Ct. 2518, 2540 (2014) ("To meet the requirement of narrow tailoring, the government must demonstrate that alternative measures that burden substantially less speech would fail to achieve the government's interests.").

40. *See* Dean Baquet & Bill Keller, *When Do We Publish a Secret?*, N.Y. Times (July 1, 2006), http://www.nytimes.com/2006/07/01/opinion/01keller.html?-auth=login-email.

41. Cohen v. Cowles Media Co., 501 U.S. 663, 669 (1991) ("[G]enerally applicable laws do not offend the First Amendment simply because their enforcement against the press has incidental effects on its ability to gather and report the news."). Note, however, that in *Bartnicki v. Vopper*, 532 U.S. 514 (2001), the Supreme Court struck down a statute that prohibited the intentional disclosure of the contents of an illegally intercepted communication. When a radio host, who had not participated in the interception of a phone call but obtained the tape from a source, broadcast the intercepted tape, one of the speakers on the tape brought a suit against the host. The Court held that the government may not punish the publication of lawfully obtained information relating to matters of public interest, even if the source who provided the information obtained it unlawfully. *Id.* at 535. In

striking down 18 U.S.C. § 2511(1)(c), the Court found it was a "content-neutral law of general applicability." *Id.* at 526. Section 793(e), as a content-based restriction, would face even greater scrutiny than was applied in *Bartnicki*.

42. *See, e.g.*, United States v. Morison, 844 F.2d 1057, 1068 (4th Cir. 1988); *see also* Branzburg v. Hayes, 408 U.S. 665, 691-92 (1972) ("It would be frivolous to assert—and no one does in these cases—that the First Amendment, in the interest of securing news or otherwise, confers a license on either the reporter or his news sources to violate valid criminal laws.").

43 Humanitarian Law Project, 561 U.S. at 18 (quoting United States v. Williams, 553 U.S. 285, 304 (2008)). *See also General Elec. Co. v. E.P.A.*, 53 F.3d 1324, 1328–29 (D.C. Cir. 1995) (holding that the government may not impose civil or criminal liability where a law or regulation "is not sufficiently clear to warn a party about what is expected of it")

44. *See Humanitarian Law Project*, 561 U.S. at at 19 (quoting Hoffman Estates v. Flipside, Hoffman Estates, Inc., 455 U.S. 489, 499 (1982))

45. *Id.* at 20

46. 18 U.S.C. § 793(e) (2015)

47. The Fourth Circuit assumed this to be true: "unauthorized possession" is tied to the government classification system. *See* United States v. Morison, 844 F.2d 1057, 1074-76 (4th Cir. 1988).

48. 18 U.S.C. § 793(e) (2015).

49. Prior to the 1950 amendments, the Supreme Court did hold that Sections 1 and 2 of the Espionage Act—the precursors to today's Sections 793-798—were not vague. Gorin v. United States, 312 U.S. 19, 27 (1941). Because Section 793(e) did not exist in its current form at the time *Gorin* was decided, and because the statute was *not* vague as to its application to the defendants in that case (a Russian-born government contractor and a foreign agent), that case is not binding here. *But see* United States v. Morison, 844 F.2d 1057, 1071-74 (4th Cir. 1988) (holding Section 793(d) is not vague, but as in *Gorin*, defendant should not have standing to argue vagueness as the statute is not vague as applied to him, a government employee); United States v. Hitselberger, 991 F. Supp. 2d 101, 107 (D.D.C. 2013) ("simple willfulness has never been held to be unconstitutionally vague").

50. *See* David Folkenflik, *Q: Could U.S. Prosecute Reporters for Classified Scoops? A: Maybe*, NPR (Mar. 22, 2017) (reporting that James Comey testified that "whether a reporter incurs criminal liability by publishing classified information" is a matter "probably beyond my ken"), http://www.npr.org/sections/thetwo-way/2017/03/22/521009791/q-could-u-s-prosecute-reporters-for-classified-scoops-a-maybe.

51. Wayte v. United States, 470 U.S. 598, 607 (1985) (citing United States v. Goodwin, 457 U.S. 368, 380, n. 11 (1982)).

52. *Id.* at 608. Note that though the Fifth Amendment does not have an equal protection clause, the Supreme Court has held the Fourteenth Amendment protections of equal protection to be encompassed by the Fifth Amendment Due Process Clause. *See* Bolling v. Sharpe, 347 U.S. 497, 499 (1954).

53. *Wayte*, 470 U.S. at 603

54. *Id.*

55. *Id.* at 604

56. *Id.* at 603.

57. *Id.* at 609

58. It is possible that journalists receiving information from the administration—i.e. with the consent of the President—are considered "authorized" for purposes of Section 793(e) even though the information may remain classified

59. Baquet & Keller, *supra* note 40.

60. *Id.*

61 Nebraska Press Ass'n v. Stuart, 427 U.S. 539, 559 (1976). The classic examples of prior restraints are "court orders that actually forbid speech activities" like restraining orders or injunctions. Alexander v. United States, 509 U.S. 544, 549–50 (1993)

62. *Nebraska Press Ass'n*, 427 U.S. at 559.

63. *See* N.Y. Times Co. v. United States, 403 U.S. 713, 733 (1971) (White, J., concurring) ("Prior restraints require an unusually heavy justification under the First Amendment; but failure by the Government to justify prior restraints does not measure its constitutional entitlement to a conviction for criminal publication.").

64. *See* Smith v. Daily Mail Pub. Co., 443 U.S. 97, 100–01 (1979).

65. Org. for a Better Austin v. Keefe, 402 U.S. 415, 419 (1971).

66. Bartnicki v. Vopper, 532 U.S. 514, 527 (2001) (quoting Smith v. Daily Mail Publishing Co., 443 U.S. 97, 102 (1979)).

Overclassification Meets the Constitutional Access Right

ANDREW UDELSMANN

> "History teaches us how easily the spectre of a threat to 'national security' may be used to justify a wide variety of repressive government actions. A blind acceptance by the courts of the government's insistence on the need for secrecy, without notice to others, without argument, and without a statement of reasons, would impermissibly compromise the independence of the judiciary and open the door to possible abuse."
>
> *In re Washington Post Co.*, 807 F.2d 383, 391-92 (4th Cir. 1986).

Overclassification is a growing problem that continues to corrode the ability of the U.S. press and public to monitor the actions of their government. In 2014 alone, Executive agencies classified 77,562,436 records.[2] That classification is meant to signify that some level of harm to national security "reasonably could be expected" to result if the records were made public.[3] In reality, many of these documents could be disclosed without any risk to national security whatsoever. As President Obama admitted in defending Hillary Clinton's mishandling of "classified" information: "There's classified, and then there's *classified*."[4]

In *Husayn v. Mattis*, Yale Law Schools' Media Freedom and Information Access (MFIA) Clinic[5] is acting on behalf of a Pro Publica reporter to challenge overclassification in a rather novel context. MFIA was created in 2009 to support the essential work of investigative journalists and to promote government accountability. It is pursuing access to classified records filed in *Husayn* as part of the clinic's Constitutional Access project, which seeks to enforce and expand the public's First Amendment right of access to government proceedings and related records.[6]

MFIA asserts in *Husayn* that courts violate the public's First Amendment right of access to judicial records when they seal records containing information "classified" by the Executive branch, without independently assessing whether the constitutional standard governing court access has been satisfied.[7] Simply deferring to the Executive's classification determinations violates Constitutional separation of powers, contravenes Supreme Court precedent, and creates a situation ripe for abuse.

The Scourge of Overclassification

Overclassification is not a new phenomenon. In 1997, Senator Patrick Moynihan chaired a "Commission on Protecting and Reducing Government Secrecy" to investigate the executive's procedures of classifying information. The resulting report found that "[s]ome two million Federal officials, civil and military, and another one million persons in industry, ha[d] the ability to classify information."[8] The report discussed at length the dangers of overclassification, which it described as "detrimental to both our democracy and our security."[9] The Commission's conclusion was clear: "There needs to be some check on the unrestrained discretion to create secrets. There needs to be an effective mode of declassification."[10]

Unfortunately, there has been no such check. The number of classified documents has grown exponentially since 1997, and the government's attempt to implement meaningful declassification procedures has failed.[11] Today, somewhere between 50 percent[12] and 90 percent[13] of "classified" information is improperly so designated. That percentage varies depending on the topic—the entire field of cyber warfare, for example, is "hideously overclassified," according to former NSA director Michael Hayden.[14]

Though Executive branch officials are wont to portray overclassification as unintentional, senators with access to classified information have opined otherwise. After calling for declassification of evidence that Russia interfered with the 2016 election, for example, a senator on the Intelligence Committee—Democrat Ron Wyden—explained: "My increasing concern is that classification now is being used much more for political security than for national security."[15]

Indeed, much of the Senate Intelligence Committee's study of the CIA's harsh interrogation program—the Senate Torture Report—focused on the CIA's *intentional* misuse of its authority to classify information. The publicly released Executive Summary of that report details how the CIA selectively released classified information that suggested its "enhanced interrogation program" was effective, while withholding the overwhelming body of evidence that suggested otherwise.[16] The report alleges that the CIA intentionally used this strategy to "counter public criticism, shape public opinion, and avoid congressional action."[17] President Trump, incidentally, has expressed similar concerns.[18]

Husayn v. Mattis

Husayn v. Mattis is the habeas corpus action filed by Guantánamo prisoner Zayn al-Abidin Muhammad Husayn, more commonly known as "Abu Zubaydah." Abu Zubaydah was one of the first three Guantánamo prisoners, and the primary test subject of the CIA's torture program.[19] He plays a starring role in the Senate Torture Report, which mentions his name on 199 of the 525 pages of the disclosed Executive Summary.[20]

Abu Zubaydah filed his habeas

Andrew Udelsmann *was a student director of the Media Freedom and Information Access Clinic at Yale Law School during the 2016-17 school year. The views expressed in this article are strictly those of the author and do not purport to express the school's institutional views, if any.*

petition in the D.C. District Court in 2008, following the Supreme Court's *Boumediene v. Bush* decision holding that Guantánamo prisoners had the right to habeas corpus.[21] His petition remains pending. As of April 2016, the case appeared to have ground to a halt: at that time, there were at least fourteen unresolved motions on the docket, several of which dated back to 2009.[22] Some pending motions addressed serious issues such as the CIA's alleged destruction of evidence;[23] others were as trivial as a motion for a status conference.[24] Things had become so backed up that, somewhat ironically, one of the pending matters was a motion to recuse the then-presiding Judge Roberts for failing to act on the pending motions.[25]

Pro Publica reporter Ray Bonner wanted to investigate why the court was ignoring Abu Zubaydah's case. But systematic sealing of the docket prevented him from doing so— the vast majority of the filings on the *Husayn* docket were entirely unavailable for public inspection. On behalf of Mr. Bonner, MFIA moved to intervene and unseal records in the case last year.[26]

As MFIA demonstrated in its briefings, Mr. Bonner has a First Amendment right to inspect the records of Abu Zubaydah's habeas proceeding.[27] That right of access is implicit in the guarantees of free speech and freedom of the press.[28] As the Supreme Court recognized in *Richmond Newspapers, Inc. v. Virginia*, "guaranteed rights to speak and to publish concerning what takes place at a trial would lose much meaning if access to observe the trial could . . . be foreclosed arbitrarily."[29] While the qualified First Amendment access right initially attached only to criminal trials, the right has since been extended to other contexts, including records filed in Guantánamo habeas proceedings.[30] The systematic sealing of Abu Zubaydah's docket violated Mr. Bonner's right to inspect those records.

Shortly before MFIA Clinic filed its motion, the case was reassigned from Judge Roberts to Judge Sullivan. Four days after the motion was filed, Judge Sullivan ordered the government to file public versions of the documents Mr. Bonner requested, without even waiting to hear from the government.[31] Only then did the government finally post public versions of the previously unavailable filings.

Yet many of the newly released records contain pages upon pages of bizarre redactions. For example, a report from the International Committee of the Red Cross appears on the docket twice as exhibits. In the first instance, the report is released in full;[32] in the second, it is completely redacted.[33] To take another example, the public version of Abu Zubaydah's amended petition for writ of habeas corpus contains inexplicable redactions to publicly available information, including the deletion of a direct quotation from a 2007 *Washington Post* article.[34]

In responding to MFIA's unsealing motion, the government justifies the factual basis for its redactions in lengthy declarations from Executive officials. But those declarations are in themselves classified—the FBI's 25-page declaration is completely redacted except for the page numbers.[35] The CIA went even further by submitting its declaration *ex-parte* to the court—presumably because even the number of pages in the CIA's declaration is "classified."[36]

The government's legal argument for withholding information from court records is that the Executive Branch has "exclusive control over classified information."[37] But, as President Trump learned after federal courts struck down his two travel bans, courts have a role to play even within the realm of national security. When the Executive takes actions that burden individuals' rights guaranteed under the Constitution, the judiciary must decide if the intrusion into those rights is warranted. Where the First Amendment access right applies to court records, the Clinic contends, courts must decide whether disclosing classified information would result in a "substantial probability" of harm to a compelling interest.[38] That standard is not automatically met when documents are classified, because documents can be classified if some harm "reasonably could be expected" to result from disclosure,[39] a far lower standard than the "substantial probability" of harm required to deny the constitutional access right. Thus, even assuming that information is properly classified, classification is not in itself sufficient to overcome the First Amendment access right.

Of course, courts should afford deference to executive classification decisions—the question is how much difference. In the ongoing *Husyan* case, MFIA Clinic concedes that *substantial* deference is warranted, but cautions that "deference is not equivalent to acquiescence,"[40] and, especially given the well-documented phenomenon of overclassification, courts should review the government's redactions with a degree of skepticism. At the very least, courts should require the government to present a "logical and plausible" explanation for how disclosure of the information in question could harm national security.[41] In a similar context, another D.C. district court held just that in *Dhiab v. Obama*,[42] but the D.C. Circuit recently reversed on factual grounds. Unfortunately, the panel's three fractured opinions provide no precedential guidance on the legal issues present in *Husayn v. Mattis*.

Dhiab v. Obama

Dhiab v. Obama began when Abu Wa'el (Jihad) Dhiab, then a Guantánamo prisoner, filed a petition for writ of habeas corpus to prevent the government from force-feeding him.[43] In support of that petition, Dhiab's attorney filed under seal a classified video recording of Dhiab being force-fed.[44] Sixteen press organizations, through counsel at Levine, Sullivan, Koch, and Schulz, intervened and moved to unseal the videos, asserting the public's First Amendment right to inspect what had become judicial records.[45]

In a courageous and well-reasoned opinion, Judge Kessler granted that motion.[46] She recognized that the qualified First Amendment right attached to the videos, and the government failed to meet its burden merely by asserting that the video was classified.[47] Although she afforded substantial deference to the CIA's assertions of harm, she found that the government's concerns either were not "rational or plausible" or amounted to little more than a "heck-

ler's veto."[48] So she ordered the classified videotape evidence to be unsealed.[49]

On appeal at the D.C. Circuit, Judges Randolph, Rogers, and Williams reversed on factual grounds, but reached no consensus on the legal issues.[50] The only issue on which the judges agreed was that the government had satisfactorily demonstrated that the government had met its burden to keep the videotapes sealed.[51] The judges reached no consensus, however, on *what* exactly that burden was, nor how much deference courts should afford to Executive classification decisions. Judge Rogers concluded that classified documents in a habeas proceeding are still subject to the qualified First Amendment right of access,[52] Judge Randolph concluded they are not,[53] and Judge Williams found the issue unclear.[54] Therefore, *Dhiab* provides little-to-no guidance as to how *Husayn v. Mattis* should be resolved.

Conclusion

The Executive's role of protecting national security does not invite the judiciary to "abdicate its decision-making responsibility to the executive whenever national security concerns are present."[55] When the Executive seeks to withhold information that is subject to the public's First Amendment right of access, the judiciary must verify that disclosing the information in question would entail a "substantial probability" of harm. Given the Executive's lax classification standards, courts cannot simply defer to the Executive's classification decisions. Unquestioning deference to a branch that routinely and systematically overclassifies information is unconstitutional.

Endnotes

2. Information Security Oversight Office, 2014 Report to the President (2015), https://www.archives.gov/files/isoo/reports/2014-annual-report.pdf (reporting 46,800 original classification decisions and 77,515,636 derivative classification decisions).

3. Exec. Order No. 13,526 § 1.2.

4. Fred Kaplan, *Obama's Secrecy Problem*, Slate.com, (Apr. 15, 2016 10:48 AM), http://www.slate.com/articles/news_and_politics/war_stories/2016/04/obama_says_too_much_information_is_classified_irony_alert.html.

5. MFIA Clinic is a program of the Abrams Institute for Freedom of Expression at Yale Law School.

6. More information about the MFIA Clinic can be found at https://law.yale.edu/mfia.

7. Brief for Petitioner-Intervenor, *Husayn v. Mattis, No. 08 Civ. 01360 (D.D.C. Nov. 7, 2016), ECF No. 436.*

8. Comm'n on Protecting and Reducing Gov't Secrecy, Report, S. Doc. No. 105-2, at xxii (1997).

9. *Id.*

10. *Id.*

11. *Compare* Information Security Oversight Office, 2015 Report to the President at 5, 7 (2016), https://www.archives.gov/files/isoo/reports/2015-annual-report.pdf (reporting approximately 53,000,000 classification *decisions in 2015) with id. at 9 (reporting approximately 40,000,000 pages declassified in 2015). "Decisions" and "pages" are completely different measurements. For example, classification of the entire 6,000-page Senate Torture Report would likely be considered one classification "decision."*

12. *See Too Many Secrets: Overclassification as a Barrier to Critical Information Sharing, Hearing Before the Subcomm. on National Security, Emerging Threats, and International Relations of the Comm. on Government Reform, 108th Cong. 263 at 82-83 (2004) (statement of J. William Leonard, Director, Information Security Oversight Office, National Archives and Records Administration).*

13. *See Stephen J. Schullhoffer, Access to National Security Information under the U.S. Freedom of Information Act* at 11 *(Pub. Law & Legal Theory Research Paper Series, Working Paper No. 15- 14) ("[M]ost assessments suggest that roughly nine-tenths of classified material does not need to be so treated." (internal quotation marks omitted)).*

14. Zero Days (Magnolia Pictures 2016) (interview with Michael Hayden).

15. E. Osnos, D. Remnick, & J. Yaffa, *Active Measures: What Lay Behind Russia's Interference in the 2016 election—and What Lies Ahead?,* The New Yorker, Mar. 6, 2017, at 43.

16. S. Select Comm. On Intelligence, Committee Study of the Central Intelligence Agency's Detention and Interrogation Program, Executive Summary, Findings and Conclusions at 8 (declassified and released Dec. 3, 2004) [hereinafter "S. Torture Report"] ("The CIA coordinated the release of classified information to the media, including inaccurate information concerning the effectiveness of the IA's enhanced interrogation techniques.").

17. *Id.*

18. Donald J. Trump, Twitter (Feb. 15, 2017 5:13 AM EST), https://twitter.com/realdonaldtrump/status/831853862281699331?lang=en ("The real scandal here is that classified information is illegally given out by 'intelligence' like candy. Very un-American!").

19. S. Torture Report, at 46.

20. *See generally* S. Torture Report.

21. 553 U.S. 723 (2008).

22. *See, e.g., Petitioner's Motion for Legible Copies of Documents Relied on by the Government, Husayn v. Mattis, No. 08 Civ. 01360 (Apr. 24, 2009), ECF No.149; Petitioner's Motion for Discovery, Husayn v. Mattis, No. 08 Civ. 01360 (Sept. 14, 2009), ECF No. 212.*

23. Petitioner's Motion for Sanctions for the Spoilation of Evidence, *Husayn v. Mattis, No. 08 Civ. 01360 (Sept. 21, 2009), ECF No. 218.*

24. Petitioner's Renewed Motion and Memorandum in Support of Request for Status Conference, *Husayn v. Mattis, No. 08 Civ. 01360 (Feb. 2, 2012), ECF No. 289.*

25. Petitioner's Motion to Recuse Judge Roberts for Nonfeasance, *Husayn v. Mattis, No. 08 Civ. 01360 (Feb. 24, 2015), ECF No. 311.*

26. Motion to Intervene and Unseal Court Records by Raymond Bonner, *Husayn v. Mattis, No. 08 Civ. 01360 (Apr. 18, 2016), ECF No. 317.*

27. Corrected Memorandum of Law

by Raymond Bonner at 10, *Husayn v. Mattis, No. 08 Civ. 01360 (Apr. 20, 2016), ECF No. 319.*

28. *Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 576-577 (1980).*

29. *Id. at 577.*

30. *In re Guantanamo Bay Detainee Litig.*, 630 F. Supp. 2d 1, 11 (D.D.C. 2009).

31. Minute Order of Apr. 22, 2016, *Husayn v. Mattis, No. 08 Civ. 01360.*

32. Motion to Intervene and Unseal Court Records by Raymond Bonner, Exhibit D, *Husayn v. Mattis, No. 08 Civ. 01360 (Apr. 18, 2016), ECF No. 317-11.*

33. Petitioner's Memorandum at 15-55, (ECF-stamped page numbers), *Husayn v. Mattis, No. 08 Civ. 01360 (June 29, 2016), ECF 353.*

34. *Compare Public Version of Amended Petition for Writ of Habeas Corpus at 30, Husayn v. Mattis, No. 08 Civ. 01360 (Oct. 28, 2016), ECF No. 433, with Dan Eggen & Walter Pincus, FBI, CIA Debate Significance of Terror Suspect at 3,* WASH. POST (DEC. 18, 2007), HTTP://WWW.WASHINGTONPOST.COM/WPDYN/CONTENT/ARTICLE/2007/12/17/ AR2007121702151_PF.HTML.

35. Respondent's Memorandum in Opposition to Motion to Unseal, Exhibit A, *Husayn v. Mattis, No. 08 Civ. 01360 (Sept. 23, 2016), ECF No. 411-2.*

36. *See Respondent's Memorandum in Opposition to Motion to Unseal at 12, Husayn v. Mattis, No. 08 Civ. 01360 (Sept. 23, 2016), ECF No. 411 (redacting pincites to the CIA declaration).*

37. *Id. at 19.*

38. *Press-Enterprise II, 478 U.S. at 13-14.*

39. Exec. Order No. 13,526 § 1.2.

40. *Campbell v. Dep't of Justice, 164 F.3d 20, 30 (D.C. Cir. 1998).*

41. *See Reply to Opposition to Motion to Intervene at 8-9, Husayn v. Mattis, No. 08 Civ. 01360 (Nov. 7, 2016), ECF No. 436.*

42. 70 F. Suppp. 3d 486, 490 (D.D.C. 2014).

43. *Dhiab v. Trump, 852 F.3d 1087, 1089 (D.C. Cir. 2017).*

44. *Id. at 1089.*

45. *Id. at 1090.*

46. *Dhiab v. Obama*, 70 F. Suppp. 3d at 490.

47. *Id. at 490, 494.*

48. *Id. at 497-504 (addressing and rejecting each of the government's concerns).*

49. *Id. at 501.*

50. *Dhiab v. Trump, 852 F.3d at 1098.*

51. *Id.*

52. *Id. at 1102 (opinion of Rogers, J.) ("Because the test accounts for the protection of national security information, the presence of [classified] information in a judicial proceeding does not crowd out the decades-old and flexible approach set forth in Press-Enterprise II.").*

53. *Id. at 1096 (opinion of Randolph, J.).*

54. *Id. at 1106-07 (opinion of Williams, J.) ("[C]hoices as to level of generality for the relevant proceedings (and between proceedings and documents), and the scope of the relevant historical inquiry, can easily be decisive. . . . Yet we have little guidance from the Supreme Court, or indeed any other, as to how to make those choices.").*

55. *In re Washington Post Co., 807 F.2d 383, 391-92. (4th Cir. 1986).*

Forum on Communications Law
AMERICAN BAR ASSOCIATION

Become Active in the Forum!

Join one of the Forum's Committees
Contact Yolanda.Muhammad@americanbar.org for information

Digital Communications Committee

The Digital Communications Committee focuses on legal and policy issues of particular relevance to digital communication services including apps, websites, and related offerings. Anyone interested in these issues is welcome to join.

Co-Chair: JOSH KING
Avvo, Inc., Seattle, WA

Co-Chair: ANDREW MAR
Microsoft Corp, Redmond, WA

Diversity Moot Court Competition Committee

This committee oversees the Forum's annual First Amendment and Media Law Diversity Moot Court Competition, now in its tenth year. The competition is designed to introduce minority law students to the practice of media law and to many of the lawyers who are active in the media law bar.

Co-Chair: RACHEL E. FUGATE
Shullman Fugate PLLC, Tampa, FL

Co-Chair: JAMES McFALL
Jackson Walker LLP, Dallas, TX

Co-Chair: ROBIN LUCE-HERMANN
Butzel Long, Bloomfield Hills, MI

In-House Counsel Committee

The In-House Counsel Committee provides an opportunity for members of the Forum who are in-house, including at media companies and insurance carriers, to network with each other and discuss issues of common interest. All in-house counsel are welcome at committee events.

Co-Chair: STEPHANIE ABRUTYN
Home Box Office Inc., New York, NY

Co-Chair: JAMES McLAUGHLIN
Washington Post, Washington, DC

Internet, Social Media and Publicity Committee

This committee promotes the Forum's activities through social media and the Forum's web pages.

Co-Chair: **LAURA LEE PRATHER**
Haynes and Boone, LLP, Austin, TX
Co-Chair: **JEAN-PAUL JASSY**
Jassy Vick Carolan LLP, Los Angeles, CA

Membership Committee

This committee oversees the Forum's membership efforts and works to retain current members, recruit and welcome new members, and improve membership numbers, while working to find ways to keep current members engaged with the Forum.

Co-Chair: CYNTHIA L. COUNTS
Duane Morris LLP, Atlanta, GA

Co-Chair: ROBB S. HARVEY
Waller Lansden Dortch & Davis, LLP, Nashville, TN

Non-Pro it and Public Interest Committee

This committee promotes opportunities for Forum members to participate in public interest activities.

Chair: DAVID A. GREENE

Electronic Frontier Foundation, San Francisco, CA

Sponsorship Committee

The Sponsorship Committee solicits, tracks and monitors sponsorship for multiple and individual conferences and programs put on by the Forum.

Chair: ROBERT P. LATHAM

Jackson Walker LLP, Dallas, TX

Teach Media Law Committee

Committee members are encouraged to attend our annual meeting, to share ideas and resources via our listserv, and to participate in the evaluation of applicants for our scholarships.

Chair: LEONARD M. NIEHOFF
Honigman Miller Schwartz and Cohn LLP, Ann Arbor, MI

Training and Development Committee

The Committee plans a one-day Media Advocacy Workshop for new media lawyers as a valuable training tool as well as an introduction to the Forum on Communications Law. The Workshop is held during the Forum Annual Conference and allows new lawyers to argue various media issues to a panel of "judges."

Co-Chair: SARAH L. CRONIN
Kelley Drye & Warren, Los Angeles, CA
Co-Chair: MARK FLORES
Haynes and Boone, LLP, Forth Worth, TX

Women in Law Committee

The Women in Communications Law Committee is made up of a diverse group of women who practice communications law across the industry – and across the country. We are a strong network of professional women who serve as a supportive resource to each other for advice, guidance, and friendship. We organize networking and educational events throughout the year to build upon our members' interests and strengths. We welcome new members at all of our events.

Co-Chair: CATHERINE ROBB
Haynes and Boone LLP, Austin, TX

Co-Chair: LESLIE PEDERNALES
Moore & VanAllen, Charlotte, NC

Young Lawyers Committee

The Young Lawyers Committee promotes the participation of young lawyers in all activities of the Forum. We seek to leverage the talents and enthusiasm of lawyers who are early in their careers. We seek to empower young lawyers to become more active in communications law events, enriched through educational opportunities, connected through networking, and enhanced through professional development.

Co-Chair: DANA R. GREEN
Levine Sullivan Koch & Schulz LLP., Washington, DC
Co-Chair: SARA BELL
PBS, Arlington, VA

Communications Lawyer
American Bar Association
321 North Clark St.
Chicago, IL 60654-7598

AMERICAN BAR ASSOCIATION
Forum on Communications Law

Nonprofit Organization
U.S.Postage
PAID
American Bar
Association

Officers, Governing Committee, and Editors 2016 – 2017

Chair
Carolyn Y. Forrest
Fox Television Stations, Inc.

Chair-Elect
David Giles
EW Scripps Co.

Immediate Past Chair
David J. Bodney
Ballard Spahr LLP

Budget Chair
James T. Borelli

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

Cynthia Counts
Duane Morris LLP

Editors

Lee S. Brenner
Kelley Drye & Warren LLP

Amanda M. Leith
NBCUniversal Media LLC

Drew Shenkman
Cable News Network

ABA Staff

Forum Director
Yolanda Muhammad
Yolanda.Muhammad@americanbar.org

Governing Committee

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

Division Co-Chairs

Eastern
Stephanie Abrutyn
Shaina Ward
Lee R. Williams

Central
Karen Flax
Natalie J. Spears
Leita Walker

Western
Lisa Rafferty
Elizabeth Ryder
Steven D. Zansberg

Communications Lawyer
Volume 33:1
Summer 2017