Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | April 2019

Members of Wiley Rein's Privacy, Cyber & Data Governance Practice are gearing up for the IAPP's Global Privacy Summit here in DC. We have a great slate of articles in this issue, along with details about our upcoming April 29 networking reception and panel discussion, and links to our just-completed March Privacy & Security webinar series.

In this issue, Kat Scott and I discuss what you need to know about biometrics laws; Bethany Corbin writes about the HIPAA privacy rule and state law; Megan Brown, Kat Scott, Boyd Garriott, and I recap the FTC's recent hearing on consumer privacy; and Lee Goodman provides the latest installment of his series on the First Amendment right to political privacy. In addition, we're launching a new "Spotlight" feature that gives our attorneys a chance to dive deeper into certain areas and their practices. Below you'll find Peter Hyun's interview with Joan Stewart her privacy practice and state privacy laws, plus Megan Brown's interview with me about the FTC's approach to privacy.

We also include an invitation below to our networking reception and panel discussion on April 29, in advance of the IAPP summit, and links to our webinar series on a wide range of cutting-edge privacy and security issues. Please reach out to any of us if you have questions or comments on any of these topics, and let me know if there are other topics that you'd like to see covered in future issues. I can be reached at 202.719.4533 or dpozza@wileyrein.com. Thank you as always for reading.

—Duane Pozza, Partner, Privacy & Cybersecurity Practice

ALSO IN THIS ISSUE:

Biometrics Laws Are on the Books and More Are Coming: What You Need to Know

By Duane C. Pozza and Kathleen E. Scott

A fingerprint, a retina scan, a voiceprint or facial scan – companies increasingly collect these and other biometric identifiers in the course of doing business, and the technology to collect and use them is developing rapidly. Policymakers and regulators from DC to state capitals have been grappling with whether and how to regulate the collection, use, and sharing of biometric identifiers, with the result that

continued on page 2

Continued from page 1

some laws are already on the books – and being actively enforced – while other states are considering similar laws. As companies increasingly turn to biometrics for purposes like improving security and convenience, they need to understand what privacy laws apply and what may be on the horizon.

Why is biometric privacy being regulated?

Although there is no agreed upon definition, in general, when policymakers and regulators discuss biometric data, they are concerned generally with data that is "biologically unique to [an] individual" and that is immutable.[1] As discussed below, different jurisdictions have defined biometrics in different ways for purposes of privacy laws.

The benefits of using biometric data can be extensive. One key example is using biometrics for authentication, which has security advantages over password-based authentication systems that are susceptible to a number of vulnerabilities.[2] As one observer has described – "[b]iometric authentication is simple for people to use and can streamline previously burdensome routine processes. These aspects, in combination with the difficulty it takes to mimic, make biometric authentication an attractive asset to multiple industries."[3] Indeed, the government – at both the state and federal level – promotes the use of biometric data for authentication purposes. For example, in a 2016 report, the California Attorney General's Office specifically lamented password-based authentication systems and guided organizations to "protect access to critical systems and sensitive data" with multi-factor authentication, which "pairs 'something you know,' such as a password or PIN, with 'something you have,' ... or ***'something you are,' such as a biometric like a fingerprint.'***"[4] The federal government, including the National Institute of Standards and Technology (NIST) and the Federal Trade Commission (FTC), also has promoted biometrics for increased security.[5]

Biometric data also allows for various efficiencies – from employee time-clocking to airport security. And the use of biometric data in the health care space is promising – "[b]iometric screening ... can help identify health risk factors ... improve health outcomes and decrease health disparities."[6]

At the same time, there are important privacy concerns regarding the collection and use of biometric data. One important concern is that biometric identifiers are immutable, and as a result, the stakes are high regarding any security breach. As the Illinois legislature explained in passing its biometric privacy bill: "Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[7]

State laws

At the state level, there are a variety of ways that legislators are addressing biometric privacy, including through:

- ***Omnibus privacy laws***, like the California Consumer Privacy Act (CCPA)[8] that sweeps in biometric data in its broad definition of "personal information;"
- ***Biometrics privacy laws***, like those in Illinois,[9] Texas,[10] and Washington,[11] that create specific notice, consent, security, and other requirements for the collection, use, and sharing of biometric data; and
- ***Breach notification laws***, like those in Arizona,[12] Colorado,[13] Delaware,[14] Iowa,[15] Illinois,[16] Louisiana,[17] Maryland,[18] Nebraska,[19] New Mexico,[20] North Carolina,[21] Oregon,[22] South Dakota,[23] Wisconsin,[24] and Wyoming,[25] which all include biometric data as a data

continued on page 3

Continued from page 2

element that triggers notification requirements in the event of a data security breach.

These laws all treat biometric privacy and security in different ways. For example, just looking at the three biometric-specific laws, they differ in scope in important ways:

- **What data is covered?** Each law has its own variation on what data it covers, and how that covered data is defined. Illinois defines a "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[26] The Illinois law also covers "biometric information," defined as "any information, regardless of how it was captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."[27] Washington defines "biometric identifier" to mean "data generated by automatic measurements of an individual's biological characteristics, such as fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual."[28]
- **What uses of that data are covered?** State laws differ on this point as well. In Illinois, for example, obligations are triggered by merely being in possession of or collecting the covered data.[29] Washington's law, however, is not as broad in scope. That law generally imposes obligations for "enroll[ing] a biometric identifier in a database for a commercial purpose," and makes an explicit exception for uses of the data that are in furtherance of a security purpose.[30]
- **What type of notice and consent requirements does the law impose?** Each of the laws imposes notice and consent requirements, but they differ as well. In Illinois, notice and consent both need to be written.[31] Washington, on the other hand, makes clear that "[t]he exact notice and type of consent required to achieve compliance with [the notice and consent requirement] is context-dependent."[32]
- **Are there restrictions on transferring the data to a third party?** Texas, for example, restricts "[a] person who possesses a biometric identifier of an individual that is captured for a commercial purpose ... [from] sell[ing], leas[ing], or otherwise disclos[ing] the biometric identifier" outside of a limited set of exceptions.[33]
- **Are there security requirements?** These laws generally require "reasonable" security requirements. In Washington, for example, a person in possession of biometric identifiers that have been enrolled for commercial purposes "[m]ust take reasonable care to guard against unauthorized access to and acquisition of" the data.[34] Companies should also be aware of data retention or deletion requirements. In Texas, for example, an entity covered by the law must "destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires."[35]
- **How is the law enforced?** The Illinois biometrics privacy law authorizes a private right of action for violations of the law; the biometrics laws in Washington and Texas do not.
- **Is there an exception for data covered under HIPAA?** The Illinois law, for example, excludes from the definition of "biometric identifier" "information captured from a patient in a health care setting or information collected, used, or stored for healthcare treatment, payment, or operations under [HIPAA]."[36]

And even looking beyond those three laws, the definition of covered "biometric" information varies widely from state to state. For example, California defines "biometric information" very broadly to include, among other things, "keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information."[37]

continued on page 4

Biometrics Laws Are on the Books and More Are Coming: What You Need to Know

Continued from page 3

In addition to the unique obligations that these laws impose on organizations that deal with biometric data, these laws also generate increased risk of liability. For example, the private right of action in Illinois's biometrics law has opened the door for plaintiffs' lawyers to file hundreds of cases.[38] And the Illinois Supreme Court **recently decided** that under that law, there is no requirement to show actual harm, giving "its blessing to a flood of litigation, which may prove costly and deter companies from launching innovations in Illinois," as our colleagues have written.[39]

And the state laws that have already been enacted are not the end of the story. Several states are currently considering bills that address privacy concerns about biometrics – including biometric-specific privacy laws, as well as omnibus and state breach notification laws to include biometric data. For example, Florida is considering a biometrics privacy bill that models the Illinois law, complete with a private right of action.[40] California – a state that already has swept in biometric data under its omnibus privacy bill – is currently considering adding biometric data as an element of personal information under its state breach notification law.[41]

Federal efforts

At the federal level, Congress and multiple agencies **have been working on privacy legislation** and standards that would affect the collection and use of biometric information, among other types of data.

One area that has received particular attention is facial recognition. The Federal Trade Commission (FTC) has issued best practices that build upon the FTC's general privacy framework, which focuses on three main principles:

1. **Privacy by Design:** Companies should build in privacy at every stage of product development.
2. **Simplified Consumer Choice:** For practices that are not consistent with the context of a transaction or a consumer's relationship with a business, companies should provide consumers with choices at a relevant time and context.
3. **Transparency:** Companies should make information collection and use practices transparent.[42]

Additionally, the National Telecommunications and Information Administration (NTIA) has facilitated a multistakeholder process which developed a set of voluntary *Privacy Best Practice Recommendations for Commercial Facial Recognition Use*.[43] The principles highlighted by the NTIA document are transparency; developing good data management practices; use limitation; security safeguards; data quality; and problem resolution and redress.[44] And just like at the state level, there may be more to come in this Congress, bipartisan legislation on facial recognition – the Commercial Facial Recognition Privacy Act – is among the privacy proposals being considered.[45]

Moving Forward

The bottom line is that for companies dealing with biometric data – or those considering doing so – the landscape is complicated. There are evolving expectations and obligations, and growing liability risk. At the same time, the beneficial uses of this data – including for security use cases – are potentially enormous and have been encouraged in other contexts. It is critical for companies to be familiar with the current laws and guidance and pay attention to laws that may be on the horizon. ▪

For additional information, please contact:

Duane C. Pozza
dpozza@wileyrein.com
202.719.4533

Kathleen E. Scott
kscott@wileyrein.com
202.719.7577

Endnotes

[1] *See* 740 ILCS § 14/5.

continued on page 5

Continued from page 4

[2]Thomas B. Pahl, Acting Director, FTC Bureau of Consumer Protection, *Stick with Security: Require secure passwords and authentication*, FTC (Aug. 11, 2017), **https://www.ftc.gov/news-events/blogs/business-blog/2017/08/stick-security-require-secure-passwords-authentication** ("Consumers and employees often reuse usernames and passwords across different online accounts, making those credentials extremely valuable to remote attackers. Credentials are sold on the dark web and used to perpetrate credential stuffing attacks – a kind of attack in which hackers automatically, and on a large scale, input stolen usernames and passwords into popular internet sites to determine if any of them work. Some attackers time their log-in attempts to get around restrictions on unsuccessful log-ins. To combat credential stuffing attacks and other online assaults, companies should combine multiple authentication techniques for accounts with access to sensitive data.").

[3]Alexandro Pando, *Beyond Security: Biometrics Integration Into Everyday Life*, Forbes (Aug. 4, 2017), **https://www.forbes.com/sites/forbestechcouncil/2017/08/04/beyond-security-biometrics-integration-into-everyday-life/#7884d07c431f**.

[4]California Data Breach Report, 2012-2015, **http://src.bna.com/cFY** (emphasis added).

[5]*See, e.g., Protecting Personal Information: A Guide for Business*, Federal Trade Commission (Oct. 2016), **https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf** ("The information could be further protected by requiring the use of a token, 'smart card,' thumb print, or other biometric—as well as a password—to access the central computer."); Ron Ross, et al., *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, NIST 800-171 at D-10 (June 2015), **https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-171.pdf** (calling for the use of "multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.").

[6]Alexandro Pando, *Beyond Security: Biometrics Integration Into Everyday Life*, Forbes (Aug. 4, 2017), **https://www.forbes.com/sites/forbestechcouncil/2017/08/04/beyond-security-biometrics-integration-into-everyday-life/#7884d07c431f**.

[7]*See* 740 ILCS § 14/5.

[8]CCPA 1798.140(o)(1)(E).

[9]740 ILCS § 14/.

[10]Tex. Bus. & Com. Code § 503.001.

[11]Wash. Rev. Code § 19.375.

[12]Ariz. Rev. Stat. § 18-551(11)(i).

[13]Colo. Rev. Stat. § 6-1-716(1)(a), (g).

[14]Del. Code tit. 6, § 12B-101(7).

[15]Iowa Code §§ 715C.1(11)(a)(5).

[16]815 ILCS §§ 530/5.

[17]La. Rev. Stat. §§ 51:3073(4)(a)(v).

[18]Md. Code Com. Law §§ 14-3501(e)(1)(i)(6).

[19]Neb. Rev. Stat. §§ 87-802(5).

[20]N. M. S. A. 1978, § 57-12C-2(A), (C).

[21]N.C. Gen. Stat §§ 75-61, 14-113.20(b).

[22]Oregon Rev. Stat. §§ 646A.602(11).

[23]S.D. Cod. Laws §§ 22-40-19(4).

[24]Wis. Stat. § 134.98(b).

[25]Wyo. Stat. § 6-3-901(b).

[26]740 ILCS § 14/10. Texas has a near-identical definition: "retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry." Tex. Bus. & Com. Code § 503.001(a).

[27]740 ILCS § 14/10.

[28]Wash. Rev. Code § 19.375.010(1).

[29]740 ILCS § 14/15.

30Wash. Rev. Code § 19.375.020(1).

[31]740 ILCS § 14/15(b).

[32]Wash. Rev. Code § 19.375.020(2).

[33]Tex. Bus. & Com. Code § 503.001(c)(1).

[34]Wash. Rev. Code § 19.375.020(4)(a). *See also* Tex. Bus. & Com. Code § 503.001(c)(2) ("A person who possesses a biometric identifier of an individual that is captured for a commercial purpose ... shall store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the person stores, transmits, and protects any other confidential information the person possesses.").

[35]Tex. Bus. & Com. Code § 503.001(c)(3) (includes exceptions).

[36]740 ILCS § 14/10.

[37]CCPA 1798.140(b).

[38]*See* Ben Koch, *Ill. High Court Sides With Consumers in Biometric Privacy Suit*, Law360 (Jan. 25, 2019), **https://www.law360.com/appellate/articles/1122073**.

[39]Megan Brown and Boyd Garriott, *Illinois: Actual Injury Not Required for Privacy Lawsuit; Inviting Costly Litigation against Innovators*, Wiley Connect (Jan. 25, 2019), **https://www.wileyconnect.com/home/2019/1/25/illinois-actual-injury-not-required-for-privacy-lawsuit-inviting-costly-litigation-against-innovators**.

[40]Jessica Davis, *Florida Proposes State Biometric Data Privacy Legislation,* Health IT Security (Mar. 11, 2019), **https://healthitsecurity.com/news/florida-proposes-state-biometric-data-privacy-legislation**.

[41]*See* California AB 1130, **http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1130**.

[42]*Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, Federal Trade Commission (Oct. 2012), **https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf**.

[43]*Privacy Best Practice Recommendations For Commercial Facial Recognition Use*, **NTIA, https://www.ntia.doc.gov/files/ntia/publications/privacy_best_practices_recommendations_for_commercial_use_of_facial_recogntion.pdf**.

[44]*Id.*

[45]*See* S. 847, 116th Cong. (in progress 2019-2020).

The HIPAA Privacy Rule and State Law: Evaluating Barriers to Care Coordination and Value-Based Health Care

By Bethany A. Corbin

The transition from fee-for-service to value-based health care is a priority for the U.S. Department of Health and Human Services (HHS). At the American Bar Association's 20th Annual Emerging Issues in Healthcare Law Conference, held March 13-16, 2019, Department of Health and Human Services Deputy Secretary Eric Hargan explained that while the health care system is moving toward value-based care, progress has not been as rapid as necessary. According to Deputy Secretary Hargan, the transition to value-based health care has been slower than anticipated due to the need to reorient the entire health care system and holistically evaluate all health care policies and programs. As part of this effort, HHS is evaluating long-standing health care laws and regulations – 85% of which haven't been updated in more than 25 years – with a view toward understanding why the laws were enacted and what they've accomplished. A significant goal is to enhance care coordination, with a focus on outcomes-based incentives and improved information sharing.

HHS REQUEST ON "BARRIERS"

Care coordination, a critical component of value-based health care, requires that patients be able to seamlessly transfer their records and health care data between numerous providers and service organizations. To better encourage care coordination, and as part of the ongoing evaluation of health care regulations, the Department of Health and Human Services' Office for Civil Rights (OCR) published a request for information (RFI) seeking to identify provisions of the Health Insurance Portability and Accountability Act (HIPAA) that operate as a barrier to information sharing and hinder the transition to value-based health care.[1] Underlying the RFI was OCR's concern that the HIPAA Privacy Rule may place unnecessary burdens on the ability of covered entities and business associates to effectively and legally transfer patient information to coordinate care and manage illnesses. In particular, OCR noted that covered entities have "expressed reluctance" to share protected health information (PHI), due to the penalties associated with violations of the HIPAA Privacy Rule.[2] The RFI comment period closed on February 12, 2019, and OCR received over 1,300 comments.[3]

While OCR's analysis of the Privacy Rule is well-intentioned, it is questionable whether the Privacy Rule is primarily to blame for reduced information sharing and care coordination.[4] In general, the HIPAA Privacy Rule enables information sharing and does not impede the distribution of PHI for care coordination purposes. The bedrock principle of the Privacy Rule is that a covered entity or business associate may not use or disclose PHI except as expressly permitted by the Privacy Rule or as authorized by the patient in writing.[5] The Privacy Rule only requires disclosure under two circumstances: (1) to the patient herself upon request in accordance with 45 C.F.R. §§ 164.524 and 164.528, and (2) to the Department of Health and Human Services as part of a compliance investigation or enforcement action.[6] Although the required disclosures of PHI are purposefully limited, the Privacy Rule sets forth numerous categories of permissible disclosures, which can be used to enhance care coordination without the patient's authorization. Indeed, a key component of the Privacy Rule is to ensure that health care providers and insurers can use and disclose information to accomplish the underlying core activities of the health care system.

As such, the Privacy Rule expressly permits covered entities to use and disclose PHI for treatment, payment, and health care operations (TPO). The Privacy Rule is clear that "treatment" encompasses disclosure to prospective downstream health care

continued on page 7

Wiley Rein Spotlight Interview: Joan Stewart on State Privacy Laws and Compliance

In this Spotlight, partner Peter Hyun interviews of counsel Joan Stewart about her privacy practice and state privacy laws and compliance.

Peter: Let's say I'm a fast-growing web-developer who has created an app that accesses personal data on a customer's smartphone, and I am looking for privacy-related advice. How can you help me?

Joan: I help clients determine whether and how various privacy laws and regulations apply to their business, and then help them design and implement compliant privacy programs. I usually work with clients to create a data flow chart to ensure that both the client and I have a full understanding of what personal data they are collecting and how they are using and sharing that data. Once we have that in place, then I help the client create policies and programs – including privacy policies, terms of service, and internal procedures – to ensure they are complying with International, Federal and State laws. In preparing for the implementation of the General Data Protection Regulation (GDPR) in the European Union, I was trained as a Certified Information Privacy Professional with a specific focus on European regulation (CIPP/E). As many of the emerging state laws are based on the concepts first adopted in the GDPR, this allows our clients to benefit from my additional training and experience in designing and implementing programs that comply with these more stringent requirements.

continued on page 9

The HIPAA Privacy Rule and State Law: Evaluating Barriers to Care Coordination and Value-Based Health Care

Continued from page 6

providers, including inpatient facilities and nursing homes.[7] Additionally, pursuant to the TPO provisions, covered entities may disclose PHI for payment purposes and health care operations, including billing and collections, risk adjustments, claim adjudication, coverage determinations, administrative activities, and quality improvement activities. Therefore, the Privacy Rule's permissible disclosure of PHI for TPO actually encourages rather than stifles information sharing between health care providers and facilities.

State Law Obstacles

That said, there is at least one aspect of the Privacy Rule that may operate as a barrier to efficient information exchange: The Privacy Rule does not preempt stricter state privacy laws. Instead, the Privacy Rule establishes a federal floor for privacy protections involving PHI maintained or held by covered entities or business associates. State laws that provide greater privacy protections or rights to individuals with respect to individually identifiable health information are not preempted by the Privacy Rule.

More restrictive state privacy laws, however, have the potential to significantly limit information flow between health care providers by prohibiting exchange for certain categories of information or imposing burdensome requirements on such information exchanges. For example, whereas the HIPAA Privacy

continued on page 8

The HIPAA Privacy Rule and State Law: Evaluating Barriers to Care Coordination and Value-Based Health Care

Continued from page 7

Rule treats all PHI equally (with the limited exception of psychotherapy notes), state laws may restrict disclosure of sensitive health information, such as that on sexually transmitted diseases, substance abuse, and mental health data without the patient's prior consent.[8] This can result in a multi-dimensional, complex web of privacy laws that creates conflicting standards regarding the use and disclosure of PHI for treatment and care coordination.

Further compounding this problem is that states may have numerous privacy laws scattered throughout different code sections or chapters, making it difficult for providers to locate relevant information and determine if PHI disclosure is appropriate. The situation becomes even more complicated for covered entities that operate in multiple states. Multi-jurisdiction providers must interpret and comply with numerous and varying state laws, which may conflict. As a result, these covered entities may adopt policies and procedures that adhere to the most restrictive state's privacy laws to minimize risk and administrative burden. Providers may therefore unnecessarily restrict PHI disclosure in states where it is legally permissible, which impedes information sharing.

Thus, to achieve OCR's identified goals in the RFI, it may be necessary to preempt state health care privacy laws – either in their entirety or partially (to the extent they create different disclosure requirements for treatment). While full preemption of inconsistent state laws would provide clear disclosure standards, greater simplicity, and consistent information sharing standards for care coordination, it likely cannot be achieved through modification of the HIPAA Privacy Rule. Rather, it would require changes to the HIPAA statute to permit preemption of state law. It is therefore important that HHS evaluate the interplay between state law, federal law, and agency regulations when analyzing how statutes and regulations may interact to promote or impede the transition to value-based care and care coordination. ▪

For more information, please contact:

Bethany Corbin
bcorbin@wileyrein.com
202.719.4418

Endnotes

[1] Request for Information on Modifying HIPAA Rules To Improve Coordinated Care, 83 Fed. Reg. 64302 (Dec. 14, 2018), https://www.govinfo.gov/content/pkg/FR-2018-12-14/pdf/2018-27162.pdf.

[2] *Id.* at 64303.

[3] *See* Request for Information on Modifying HIPAA Rules To Improve Coordinate Care, Docket No. HHS-OCR-09454-AA00, https://www.regulations.gov/document?D=HHS-OCR-2018-0028-0001.

[4] For a more in-depth discussion of this topic and opportunities for improving care coordination, see Kirk Nahra & Bethany Corbin, *USA: The HIPAA Privacy Rule – Evaluating Care Coordination and Opportunities for Improvement*, DataGuidance (Feb. 2019), https://platform.dataguidance.com/opinion/usa-hipaa-privacy-rule-evaluating-care-coordination-and-opportunities-improvement (registration required).

[5] *See* 45 C.F.R. § 164.502.

[6] *Id.*

[7] Dep't Health & Human Servs. OCR & Office the Nat'l Coordinator for Health Info. Tech., Permitted Uses and Disclosures: Exchange for Treatment 3 (Jan. 2016), https://www.hhs.gov/sites/default/files/exchange_treatment.pdf.

[8] *See* Nat'l Governors Ass'n, Getting the Right Information to the Right Health Care Providers at the Right Time: a Road Map for States to Improve Health Information Flow Between Providers 22 (July 2018), http://natlgovassoc.wpengine.com/wp-content/uploads/2018/07/1612HealthCareRightInformation.pdf.

Wiley Rein Spotlight Interview: Joan Stewart on State Privacy Laws and Compliance *Continued from page 7*

Peter: Have there been instances where you have advised clients to re-orient their entire data flow chart – or is your general approach to work with what the client's systems have?

Joan: I always try to leverage the system the client has in place. However, sometimes the existing flow must be changed to comply with privacy requirements. When I encounter those situations, I strive to identify the least invasive changes that will result in compliance.

Peter: As you are tracking the legal landscape to help clients maintain compliance and best practices, what are the trickiest privacy-related issues going forward?

Joan: The rollout of competing state privacy rules is going to make privacy compliance in the U.S. very difficult. Companies are working to come into compliance with the California Consumer Privacy Act even though many of its requirements are still subject to amendment or clarification. At the same time, other states are proposing legislation that would impose more stringent or just different obligations on companies that do business in that state. The evolving patchwork of state laws makes it tricky for companies to create a uniform compliance system or update their current system, but there are steps they can take to try to account for these different state laws.

Peter: You're a regular attendee of IAPP's Global Privacy Summit and will be in attendance later this month. What are you looking forward to at that Summit?

Joan: I always look forward to the IAPP conferences – I know I am going to come away having learned new information or been challenged to think in new ways. During the upcoming DC conference, I am particularly looking forward to the sessions on the California Consumer Privacy Act, given that the CCPA's final requirements are still in flux. I also enjoy the opportunity to meet and discuss developments with other privacy professionals. In fact, we'll be hosting a networking reception at Wiley Rein on April 29, right before the Summit.

Peter: If you look into your crystal ball, what are the key issues in privacy that you think the government and industry will be grappling with going forward?

Joan: The key issue I am watching is the obligations imposed by new privacy regulations – such as opt-in rights, deletion, or access to data – and whether existing privacy structures can accommodate these demands. For each state that considers and passes legislation, the privacy compliance framework is becoming more complicated. We actually help clients track proposed state privacy laws and consider their advocacy options. But regardless of any one state law, to be nimble enough to be responsive to these evolving privacy standards, it is crucial that any company that is collecting and using personal data embrace a privacy by design structure and be deliberate about what personal data they are collecting and how that personal data is being used and shared. ▪

For additional information, please contact:

Joan Stewart
jstewart@wileyrein.com
202.719.7438

What You Need to Know About the FTC's Hearing on Consumer Privacy

Duane C. Pozza, Megan L. Brown, Kathleen E. Scott, and Boyd Garriott

As part of the FTC's hearings on Competition and Consumer Protection in the 21st Century, the agency convened a two-day hearing on consumer privacy. The hearing featured remarks from the FTC Commissioners and numerous panel discussions by leading experts in the field. After the dust settled, the hearing revealed insights from the Commissioners and both areas of consensus and deep fault lines among privacy stakeholders. Here's what you need to know.

Remarks from the Commissioners

Chairman Simons' remarks were relatively high-level. He acknowledged the tradeoffs of privacy regulation by highlighting both the innovative technological developments that have come from intensive data use—like smart cities and self-driving cars—and the privacy risks that can come from these technologies. He again reiterated his support for the FTC's existing privacy enforcement strategy but stressed that the agency needed to do more.

Commissioner Philips **continued** to toe the line in calling on Congress to delineate the thorny value judgments of any privacy enforcement scheme, such as what constitutes a privacy harm. While he raised a wide range of economic concerns that could stem from greater privacy regulation, like chilling America's data-driven economy or disadvantaging smaller companies, he nevertheless endorsed expanding the FTC's privacy jurisdiction and enforcement authority.

Lastly, Commissioner Slaughter focused on the nuts and bolts of federal privacy legislation and its potential impacts. She expressed skepticism about the role of notice and choice in today's digital world, based on her view of the burden it puts on consumers. In terms of the FTC's role, she echoed the call for greater enforcement authority and resources, as well as rulemaking authority.

Areas of Consensus

There were a few areas that nearly everyone—from the Commissioners to privacy advocacy groups to industry stakeholders—agreed upon over the course of the two-day hearing. These included:

- **The need for federal privacy legislation.** The devils are in the details of course, but there was broad consensus for Congress to do something.
- **The FTC should be the nation's main privacy enforcer**—perhaps unsurprisingly at an FTC hearing and given the agency's longstanding role as the federal government's chief privacy cop.
- **Consumers should have choice when it comes to their privacy.** However, as we discuss below, how to give consumers meaningful choice was far from being in consensus.
- **The impact on smaller companies is a real concern.** Stakeholders are concerned that smaller companies would face greater challenges in dealing with new privacy laws, but views of the extent of that concern and how to handle it diverged.

Areas of Disagreement

Despite the high-level consensuses described above, there was a lot of daylight between stakeholders on a number of issues. These included:

- **What constitutes a privacy harm.** One panelist pointed to a general consensus that physical injury and financial loss constitute cognizable harms. However, many participants argued for a broader conception of privacy harm. Chairman Simons himself identified reputational injury as a privacy harm example, and one panelist argued that privacy harms could include a broad range of harms such as

continued on page 11

Continued from page 10

fear or anxiety. Perhaps in recognition of this disagreement, Commissioner Phillips argued that Congress should determine what constitutes harm.

- **How to give consumers meaningful choice.** Industry representatives pushed heavily for notice and choice, a longstanding privacy principle. However, privacy advocates and academics argued that notice and choice was no longer viable in today's environment. While many panelists acknowledged that any privacy tool would require consumers to shoulder some responsibility for their choices, there was no clear consensus around how much responsibility they should be given.
- **How to enforce a privacy law.** There was a sharp divide over preemption of state laws and whether privacy legislation should include a private right of action. There was also a split between ex-post versus ex-ante enforcement. Advocates for the former argued that it was more flexible and could assess actual harms, as opposed to theoretical effects. Advocates for the latter argued that ex-post enforcement would be too little too late for highly sensitive data.
- **How to balance the economic impacts.** While panelists discussed whether prescriptive privacy requirements could put smaller entities with fewer resources at a disadvantage, there was little consensus as to whether and how to resolve that issue. Some suggested carve-outs for small business, though another panelist pointed out that even small businesses could commit outsized privacy violations.

What's next? The FTC is accepting comments on this hearing through May 31, 2019. It remains to be seen what additional public steps the agency will take as part of its reconsideration of its privacy approach.▪

For more information, please contact:

Duane C. Pozza
dpozza@wileyrein.com
202.719.4533

Megan L. Brown
mbrown@wileyrein.com
202.719.7579

Kathleen E. Scott
kscott@wileyrein.com
202.719.7577

Boyd Garriott
bgarriott@wileyrein.com
202.719.4479

Wiley Rein and The Women's High Tech Coalition are excited to announce the addition of a panel discussion on proposed privacy legislation and regulation trends featuring Congressional staff members and an FTC advisor. We hope you can join us as we kick-off IAPP's Global Privacy Summit 2019!

Date | April 29, 2019
Time | Reception: 6:00 p.m. – 8:00 p.m.
Panel Discussion: 6:30 p.m. - 7:00 p.m.
Location | Wiley Rein LLP, 1776 K Street NW, Washington, DC 20006

RSVP

FEATURED PANELISTS

MORGAN KENNEDY
Attorney Advisor to Chairman Joseph Simons
Federal Trade Commission

SAM LOVE
Legislative Assistant for United State Senator Cory Gardner

MATT McMURRAY
Senior Legislative Assistant for Congresswoman Robin Kelly

Wiley Rein Spotlight Interview: Duane Pozza on the FTC's Hearing on Consumer Privacy

In this Spotlight, partner Megan Brown interviews partner Duane Pozza about his views on the Federal Trade Commission's approach to privacy.

Megan: I know you recently came to Wiley Rein from the FTC. What do you think of the FTC's latest moves on privacy?

Duane: Well, the FTC has been busy. We've been following its latest hearings on Competition and Consumer Protection in the 21st Century, including its recent two-day hearing on privacy. By the Commission's own account, the current hearings are designed to help the agency re-evaluate its approach to privacy. The agency has long been the primary privacy regulator for most of the economy –it issues reports with detailed recommendation on best practices, it engages in rulemaking in certain limited areas (like children's privacy), and it brings enforcement actions. It put out a comprehensive report on privacy practices in 2012, but it's now questioning whether technological change has undermined some of its conclusions.

Megan: Accounting for technological change is definitely a tricky issue. How does an agency like the FTC put out guidance on privacy issues when tech is constantly evolving?

Duane: It's tough. The agency often focuses on high-level principles rather than tech-specific recommendations. But consumer expectations about data-sharing change all the time, and research tends to show that consumers are willing to share certain kinds of data if it means getting ad-supported services for free. And also, data that was collected for one reason may end up being useful for other purposes – in a way that's helpful for the consumer. AI systems, for example, can analyze large sets of data for goals like improving public health, even though the data may not have been originally collected for that purpose.

Megan: What about enforcement? Some argue that the FTC has gone too far in bringing privacy and data security actions where it's not clear that consumers have actually been injured by the alleged law violation.

Duane: The current Commission, led by Chairman Simons, has reiterated that it will "vigorously" enforce the law in the areas of privacy and data security. Privacy cases are often based on a theory that consumers have been deceived by a privacy policy or other statements about what information will be collected and shared. Data security cases often involve actions against a company that has suffered a breach, based on a theory that the company had "unreasonable" data security practices. The Chairman has noted that injury in these cases can be hard to quantify, but it appears the Commission will continue to pursue them.

Megan: What other issues has the FTC signaled that it will take up in the near future?

Duane: The FTC has always focused on deceptive advertising, and it has signaled that it will look much

continued on page 14

Wiley Rein Spotlight Interview: Duane Pozza on the FTC's Hearing on Consumer Privacy *Continued from page 13*

more closely at social media, particularly when it comes to properly disclosing endorsements. It's also stepped up enforcement in the area of financial technology – fintech – where it can enforce consumer protection laws against non-bank companies involved in financial practices. In fact, the agency is currently considering whether to impose additional data security requirements on those companies, under its Safeguards Rule.

Megan: Many of the bills proposed in Congress would give the FTC more power in the area of privacy. If that happens, how do you think the FTC would use that power?

Duane: There does seem to be a trend in proposed federal legislation of giving greater authority to the FTC, though the scope of that varies by the bill. The Chairman has suggested that if the FTC is given greater rulemaking authority, it should be directed to implement what Congress wants, rather than rulemaking that would require the agency to make a bunch of complicated policy judgments and trade-offs. But, what Congress does remains to be seen. The agency certainly wants more funding, greater authority over certain entities like common carriers and nonprofits, and greater authority to impose penalties. If those end up included in any federal legislation, you can expect even more FTC policing on privacy and security issues in sectors all across the economy.▪

For additional information, please contact:

Duane C. Pozza
dpozza@wileyrein.com
202.719.4533

Events & Speeches

Out Go the Lights: Critical Infrastructure Threats
2019 AccessData User Summit
Matthew J. Gardner, Speaker
April 10, 2019 | Henderson, NV

Strange Bedfellows: The New Age of PBM Contracting and Effecting Investments in Downstream Entities
The Blue Cross Blue Shield 2019 National Summit
Dorthula H. Powell-Woodson, Speaker
April 29, 2019 | Grapevine, TX

Beyond Cyber Compliance: Cybersecurity as Contract Award Evaluation Criteria
PSC Annual Conference
Megan L. Brown, Speaker
April 29, 2019 | White Sulphur Springs, WV

Roundtable Luncheon with FTC Commissioner Noah Joshua Phillips
Hosted by Wiley Rein LLP
May 16, 2019 | Washington, DC | 12:30 P.M.

Government Officials on Governing Emerging Technologies
Arizona State University, Sandra Day O'Connor College of Law
Megan L. Brown, Moderator
May 23, 2019 | Phoenix, AZ

The Legal Ethics of Email and Social Media
The American Health Lawyers Association
Dorthula H. Powell-Woodson, Speaker
June 24, 2019 | Boston, MA

The First Amendment Right to Political Privacy, Chapter 7 – In Need of Judicial Clarity

By Lee E. Goodman

Introduction

Since 1950, the First Amendment has protected the political privacy of people as diverse as free marketer Edward Rumely, Marxist economist Paul Sweezy, social activist Manuel Talley, and average citizen Margaret McIntyre. It has protected associations such as the NAACP, the Jehovah Witnesses, the Committee for Constitutional Governance, the Progressive Party of New Hampshire, and the Socialist Workers Party. The diversity of citizens and causes that have invoked the privacy afforded by the First Amendment underscores why courts should resist viewing First Amendment challenges in the light of contemporary political biases and instead approach each case with political and ideological agnosticism. Future Rumelys and Sweezys should be protected equally by the First Amendment.

Yet, lower courts today are struggling to find consistency and uniformity in the jurisprudence of First Amendment privacy and in judicial outcomes. The line between political privacy and its exceptions has become blurred. At the same time, there is a national movement seeking to expose more speakers and funders of expanding categories of speech. Lower courts have, explicitly and implicitly, shined a light on ambiguities in the jurisprudence while Supreme Court Justices Alito and Thomas have acknowledged the problem and voted to take compelled disclosure cases for the purpose of clarifying the law. This chapter identifies key issues the Supreme Court needs to clarify about the First Amendment right to political privacy, starting with first principles.

1. Is Compelled Disclosure a First Amendment Harm?

Although it may sound elementary, the Supreme Court should affirm whether the First Amendment right to political privacy and its judicial provenance remain the starting analytical point for all compelled disclosure challenges. Of what continuing force are *Sweezy*, *NAACP*, *Talley*, *McIntyre* and *Watchtower*?[1] Or have they been relegated to the museum of historical judicial relics?

Setting the table for judicial review in this way is important because many lower courts have tended to gloss over, or pay mere lip service to, the early precedents establishing the First Amendment right to political privacy. The exceptions to the right of privacy have become the presumptive starting point and the burdens have been shifted to citizens to overcome the governmental interest. Accordingly, a fundamental predicate to the proper judicial analysis of government rules compelling exposure is establishing the proper starting point.

Relatedly, lower courts disagree over the nature of the constitutional harm implicated by compelled disclosure. Some lower courts have ruled that compelled disclosure of certain subjects or categories ("realms") of speech or association simply does not harm First Amendment rights.[2] The Ninth Circuit, for example, imposed upon The Center for Competitive Politics,[3] a nonprofit organization that engages in no electoral activity, a threshold burden of proving that its donors were subjected to economic reprisals, harassment, threats, or some other actual chill in order to state a *facial* claim of First Amendment infringement.[4] That is, exposure laws cause constitutional harm sufficient to put the government to its burden of justifying the exposure *only if* the plaintiffs can first prove a demonstrable chill that deters speech or membership.[5]

But the Supreme Court has not required citizens to prove harassment or retaliation in order to invoke the protection of the First Amendment in facial challenges in *Talley*, *McIntyre*, and *Buckley v. Valeo*. *Buckley* shifted the burden only for a plaintiff to justify an *as-applied* "exception" to the disclosure regime that the Court, in the first instance, found facially

continued on page 16

Continued from page 15

justified by the governmental interest in disclosure of contributions to candidates and expenditures explicitly advocating the election of candidates. The Fourth Circuit appears to have followed this approach, ruling on the facial constitutionality of a state campaign finance disclosure law while assuming a constitutional harm rather than shifting the burden to the plaintiffs to prove harassment.[6]

If there indeed exists a fundamental right to political privacy in speech, access to information, association, belief, and the right to vote, however, then any compelled disclosure would seem to infringe that right and constitute constitutional harm. If so, the Court needs to instruct lower courts that the citizen's right to political privacy and secrecy is an important right in all cases, compelled disclosure is the *per se* harm, and it is the government's burden to justify infringement of the right.

2. Are There Distinct Subjects or Categories of Anonymous Political Speech or Association That Are Off Limits to Compelled Disclosure?

The legal analysis in lower courts sometimes confuses distinct subjects of political speech or categories of political association as unprotected when the real question seems not whether the activity is protected, but whether the government's interests and impositions are sufficient to infringe upon the right. It is important not to blur the distinction between the existence of the right, whatever the subject of the speech or association, versus the governmental interest that might attach to varying speech subjects. Accordingly, the Court should do two things very clearly. First, it should identify any sacred subjects or categories of speech and association. Second, it should instruct lower courts which subjects or categories of speech and association are subject to overriding governmental interests.

For example, *Buckley* held that the government can compel exposure of the identity of a campaign's donors. The Court acknowledged that this exposure invades the right to political privacy, but found the government's interest in compelling the exposure overrides the right because the unique associational activity at issue, financial contributions to candidates, can corrupt politicians; disclosure retards corruption; and the public has a right to know to whom politicians are beholden. *McConnell* and *Citizens United* extended disclosure to "electioneering communications," issue messages that reference candidates over broadcast media within close proximity to an election.[7]

But *McIntyre* held the government cannot compel exposure of the identity of a person funding pure issue speech on a local tax referendum, because it infringes the right of the speaker anonymously to advocate a public policy, which cannot be corrupted in the way a politician can. In both contexts, the Court acknowledged the First Amendment right at stake. What differed was the subject matter of the political speech and the government's varying interests in compelling disclosure of the different subjects.[8]

Lower courts, however, are increasingly blurring any distinction between these realms of speech and association, stretching election financing disclosure precedents like *Buckley*, *McConnell*, *Wisconsin Right to Life*, and *Citizens United* to justify disclosure of issue speech and non-electoral association. *McConnell*, for example, ruled that the government could compel the disclosure of those paying for a broadcast advertisement referencing a candidate within 60 days of an election, known as an "electioneering communication," on a communication-by-communication basis, because such communications arguably influenced elections.[9] The Third Circuit has invoked *McConnell* to permit Delaware to compel nonprofit educational organizations to disclose donors over a four-year period if they incur just $500 to post the voting records of public officials on the Internet within 60 days of an election.[10] The Ninth and Second Circuits without blinking have cited *Citizens United*'s analysis of campaign finance disclosure to wholly non-electoral charitable donor disclosure.[11]

continued on page 17

Continued from page 16

Likewise, the Court should reason with precision when it does recognize a realm or context of legitimate compulsory exposure. For example, *Doe v. Reed*[12] ruled that signing a petition to invoke a public ballot procedure was indeed protected by the First Amendment, but compulsory exposure of the names of petition signators was justified because the signature activity was public in nature. The signatures were signed for the specific purpose of giving them to the government to activate a public procedure. Further, public access to the signatures advanced the government's interest in ensuring the validity of the signatures so submitted. The context mattered significantly. Yet, the Ninth Circuit has cited *Doe* as the anchor for its analysis in nonprofit donor disclosure.[13] And now the Ninth, Second, and Third Circuits are citing each other.

Therefore, it is important for the Court to identify distinctions between political subjects and associational purposes that are beyond legitimate governmental interests. The Court should clearly distinguish any sacred realms of political speech and association particularly to head off the misapplication of the campaign finance exception to political privacy.

Moreover, lower courts often conceive of certain realms of speech as wholly unprotected, rather than understanding them to be protected but subject to an exception in light of a sufficient governmental interest. Such analysis can yield careless expansions of prior Supreme Court rulings. As noted above, *McConnell* is often invoked as a *carte blanche* predicate for federal and state legislative efforts to vastly expand exposure from the narrow "electioneering communication" concept and communication-specific reports to a far broader sphere of issue advocacy and far more intrusive reporting.[14]

Indeed, no realm of speech and association is in greater need of clarification than discussion of political issues. This category includes discussion of public policies that reference the public officials who are responsible for those policies. The zone for anonymous discussion of issues and association around issues, financially or otherwise, should be clearly delineated. If a zone of speech is qualified, the Court should draw clear and unmistakable lines around which speech is – although protected – susceptible to compelled disclosure. If the protection afforded anonymous issue speech is conditioned upon context, such as the petition signatures in *Doe v. Reed*, the Court should be precise in establishing those boundaries. If the answer depends upon how the speech and association are facilitated, such as communication over publicly owned airwaves or pamphlets or electronic posts over the Internet, the Court should make that clear too.[15]

And if there are realms of speech which are off limits to compelled exposure, sacred zones, the Court needs to say so in unmistakable terms. Is pure issue speech over the Internet, for example, so far beyond the public interest that the government cannot force disclosure of its speakers? National clarification – particularly for issue speech – is needed.

3. Is It Always the Government's Burden to Justify an Infringement?

As noted above, some courts have shifted the burden to the citizen to prove harassment or retaliation in order to state both facial and as-applied First Amendment infringement claims.[16] But the Supreme Court has not insisted upon such proof to establish a facial infringement in a number of cases.[17] Harassment or retaliation should be relevant only in an as-applied challenge to a disclosure law that the government has justified facially. But even there, the government still bears the burden of justifying the as-applied burden. Therefore, the burden must always be upon the government to justify compulsory exposure of private political belief, speech and association, in both facial and as-applied challenges.

4. What Judicial Scrutiny Applies to Compelled Disclosure?

The Court consistently has used the term "exacting scrutiny" to analyze compelled disclosure laws. In *Davis v. Federal Election Commission*, a decision

continued on page 18

Continued from page 17

written by Justice Alito, the Court reaffirmed an "exacting scrutiny" standard described as follows:

> [W]e have closely scrutinized disclosure requirements, including requirements governing independent expenditures made to further individuals' political speech. To survive this scrutiny, significant encroachments cannot be justified by a mere showing of some legitimate governmental interest. Instead, there must be a relevant correlation or substantial relation between the governmental interest and the information required to be disclosed, and the governmental interest must survive exacting scrutiny. That is, the strength of the governmental interest must reflect the seriousness of the actual burden on First Amendment rights.[18]

Notwithstanding these words on a page in *Davis*, however, the true meaning of "exacting scrutiny" remains elusive and open to manipulation in implementation. Did the Court mean to suggest, for instance, that the test is a sliding scale or balancing test? That is, must the strength of the governmental interest increase to a compelling level if the invasion of privacy is severe, while a simple interest will suffice if the invasion of privacy is academic? If so, does "seriousness" testing suggest that not all invasions of political conscience constitute a First Amendment harm? And how should courts distinguish between "serious" versus "non-serious" invasions of a citizen's political privacy? Should courts decide the seriousness by some objective measure? Or is a court to shift the burden of proof to a citizen to convince the court of the "seriousness" of the invasion into its political privacy before the government even needs to justify its intrusion? What benchmarks apply to the citizen's proof?

The jurisprudence leading up to *Davis* suggests that "exacting scrutiny" was a standard very close to "strict scrutiny." Early case law required a "showing of 'overriding and compelling state interest' that would warrant intrusion into the realm of political and associational privacy protected by the First Amendment."[19] Ten years later *Buckley* cited the "strict test" of *NAACP*.[20] Since then the Court has held that, where a law burdens First Amendment rights, "exacting" and "strict" judicial review "are one and the same."[21]

Lower courts historically applied "exacting scrutiny" as the functional equivalent of "strict scrutiny."[22] More recently, however, lower courts have concluded the two scrutiny tests are quite different under the guidance of later decisions such as *McConnell* and *Citizens United*.[23] Lower courts are diluting the standard by applying a very forgiving review akin to rational basis review.[24] The Third Circuit has in effect equated exacting scrutiny with rational basis review with a high degree of judicial deference to the government's chosen means of disclosure so long as the means are merely "rationally related" to the government's objective.[25] The Second Circuit described "exacting scrutiny" as just another term for "intermediate scrutiny" and proceeded to defer to the government's proffered interests,[26] without a factual hearing. The Ninth Circuit has applied *Davis* as a sliding scale test or balancing test, requiring the citizen first to prove "actual burdens" and, based upon the severity of those burdens, then deciding the necessary strength of the government's interest, even in a facial challenge. The D.C. Circuit has acknowledged confusion between "strict" and "exacting" scrutiny, but concluded the difference is merely semantic. "In many respects, this debate over the appropriate adjective is beside the point. Whatever the test is *called*, the [Supreme] court as already described what the test *is*." The D.C. Circuit then quoted *Davis* without further elaboration because it held a disclosure law at issue satisfied strict scrutiny in any event.

Justice Thomas, the strongest voice on the Court for political privacy, has opined that only "strict scrutiny" can apply to compelled exposure of citizens exercising First Amendment rights.[27] Offended by the Third Circuit's approval of Delaware's sweeping

continued on page 19

Continued from page 18

compulsory exposure regime for the publication of voting records online, as well as the Court's denial of certiorari, Justice Thomas admonished that the case revealed how "exacting scrutiny" as effectively devolved to "no scrutiny at all."[28]

Compelled disclaimers represent another area of confusion when choosing which level of scrutiny to apply. "Disclaimers" are compulsory sponsor identification notices printed within, or accompanying, political messages. When compelled disclosure takes the form of a disclaimer identifying the speaker, the Court has treated that kind of disclosure as a form of *content-based* speech regulation, because it forces the speaker to include information she otherwise would not choose to say. Content based speech restrictions typically trigger "strict scrutiny."[29] One federal district court recently expounded at length upon the lack of clarity in this area and chose "strict scrutiny" as the appropriate test.[30]

Forcing a speaker to identify herself in a disclaimer printed on the face of a pamphlet (*Talley*, *McIntyre*), on a name badge (*American Constitutional Law Foundation*), in a public registration and report (*Watchtower*), or in response to a congressional subpoena (*Rumely*, *Sweezy*) all represent comparable invasions of privacy. Thus, while variations in mechanisms might be relevant to a tailoring analysis (see below), all compulsory speaker identification mechanisms should receive the same level of scrutiny. Regardless of whether that level of scrutiny is called "strict scrutiny" or "exacting scrutiny," the scrutiny should be a *high, rigorous level of scrutiny* for all disclosure mechanisms. Certainly, the precedents have established that the government cannot interfere with the right to speak or associate anonymously *lightly*. Likewise, wide variances in the level of scrutiny for compelled disclosure versus other kinds of infringements of First Amendment rights seems illogical, for the Court has long recognized that speech can be impeded or silenced by a wide variety of subtle government actions. The issue cries out for clarification given explicit confusion observed by lower courts. Most importantly, it is imperative that the Court clarify the level of discipline that must go into "exacting scrutiny," because lower courts are applying the analysis with little rigor at all.

In sum, lower courts have struggled to select the appropriate level of scrutiny, to articulate standards for "exacting scrutiny," or to apply "exacting scrutiny" standards with consistency or rigor. Therefore, the Court needs to clarify the scrutiny applicable to compelled disclosure rules and tell us if the scrutiny level varies based on the content of speech, the mechanism of disclosure, or this severity of associational disruption. The court also needs to clarify the analytical and evidentiary scrutiny that flows from the *Davis* within and without the campaign finance disclosure context.

5. Which Governmental Interests Can Justify the Invasion of Political Privacy?

In addition to clarifying the level of scrutiny, the Court also should provide definitive guidance about the governmental interests that justify invasions of private political belief. In compelled disclosure cases, the degree of importance required of the government's asserted interest remains unclear. The Court has referred to the governmental interest necessary to justify an infringement interchangeably as "compelling" and "overriding" in some cases,[31] but "sufficiently important" in others.[32] It is possible, if *Davis* is understood as a sliding scale, that an asserted interest must be "compelling" in order to be "sufficiently important." Ironically, the Ninth Circuit has ruled that a citizen must prove an actual burden on private association is demonstrable and "substantial" in order to state a valid First Amendment claim, but the government may proffer an interest that is merely "important" to compel exposure.[33]

Early cases preceded the doctrinal development of First Amendment privacy and scrutiny tests, but laid early foundations for governmental interests that the Court has continued to draw upon. Among the governmental interests the Court has had occasion to

continued on page 20

The First Amendment Right to Political Privacy, Chapter 7 – In Need of Judicial Clarity

Continued from page 19

consider are:

- National Security – Beginning in the communist cases in the 1940s (before and after *NAACP*) courts balanced the government's asserted need to protect the democracy from subversion against Judge Prettyman's early iteration, in *Barsky* (1948), of the "private right." Courts later distinguished communist cases from civil rights cases on the basis that national security was a more compelling governmental interest than southern states' professed interest in enforcing their corporate compliance rules.
- Preventing Corruption of Elected Officials – This interest is the *sine qua non* in the field of campaign finance restrictions. *Burroughs*, the earliest of cases (1934), recognized that disclosure of campaign contributions and expenditures was a mechanism that helped prevent corruption of politicians. *Buckley* (1976) was centrally focused on preventing corruption of elected officials.
- Informational Interest – Although *Buckley* also acknowledged government's interest in providing citizens information about who was funding the elected official's ambitions – the informational interest implicitly was subordinate to the corruption prevention interest. Citizens had an interest in knowing who funded a politician's campaign because the politician might be responsive to the funder and because the citizenry could hold the politician accountable. Likewise, *Harriss* (1954) recognized the interest legislators have in knowing who is paying to lobby them as a check against corruption and undue influence. Implicit in *Harriss* and *Buckley* was the ulterior use of the information to prevent corruption and hold politicians accountable.
- Election Procedural Integrity – *Doe* (2010) and *American Constitutional Law Foundation* (1999) recognized the public's interest in ensuring the integrity of a state-sponsored election, where the citizens engage in direct democracy, which included disclosure of the identity of those citizens who activate the election machinery.
- Law Enforcement Tool – Another interest recently recognized by two courts of appeals is a law enforcement interest where the government claims it can glean internal information about a political association in order to enforce tax laws, nonprofit solicitation laws, or in one case securities fraud laws.[34] The Ninth Circuit has ruled that a state may require a nonprofit, non-electoral organization to disclose its donors to the state not because the state *needs* the information but rather for the state's mere convenience of having the information in a library in the rare event that the information might one day be useful.[35]

Courts must study these asserted interests closely to ensure they are genuine, not pretextual, and that they override a core First Amendment right for purposes other than disclosure for disclosure's sake. Two interests deserve the Supreme Court's special consideration.

First, the most problematic is the "informational interest." This interest is problematic because its logic, when placed under a microscope, often boils down to information for the sake of information, or exposure for exposure's sake, which is circular logic. Advocates of greater exposure and lawmakers increasingly invoke this generic interest to justify virtually all compulsory disclosure. It is also a boundless justification. It can be invoked to justify public exposure in almost every context because it has no logical stopping point. It is often trumpeted under the siren sounding term "transparency," or the pablum "transparency is good," which may sound like a constructive public policy, but constitutionally it amounts to nothing more than elevation of the government's policy preference for exposure over the citizen's First Amendment right to non-exposure.[36] It can be an interest that swallows the right. The Court should place clear metes and bounds on the "informational interest" and require that the

continued on page 21

Continued from page 20

information made public actually advances a specific ulterior interest such as the prevention of *quid pro quo* corruption or election integrity.

Second, the "law enforcement" interest is problematic because it often authorizes the government to collect information about citizens' political activities not for the purpose of enforcing a specific law with respect to any suspected unlawful conduct, but for the purpose of collecting information about wholly lawful and virtuous democratic activity in order to determine if the information might yield the rare unlawful activity. The government has to collect a far broader range of private information than is necessary for a case-specific investigation in order to build a haystack in order to look for a needle in that haystack. It often resembles a fishing expedition. The collection effort can be invasive and voyeuristic, especially given that government officials are partisan creatures. And the information can be abused or misused.

6. What Degree of Tailoring Between the Government's Objective and Its Disclosure Mechanism Is Necessary to Uphold Compulsory Disclosure?

Next, courts have been all over the board in applying the standard for tailoring. *McIntyre* stated that the Court will "uphold the restriction [compelled disclosure] only if it is narrowly tailored to serve an overriding state interest."[37] Previously, the Court had stated that "[p]recision of regulation must be the touchstone in an area so closely touching our most precious freedoms."[38] Other courts have used the language of "substantial relationship" between compulsory disclosure and the asserted objective.[39] We know that disclosure only "tenuously related" to the state's asserted objective is inadequate, but after six decades of jurisprudence, we still are unclear on the degree of tailoring that is adequate.

Finally, it is unclear whether the government must choose the narrowest means of infringement in order to compel disclosure of speakers and associations. Many disclosure schemes demand far more disclosure than is necessary to prevent corruption or validate the bona fides of a nonprofit organization. Overbroad disclosure unnecessarily exacerbates the degree of the First Amendment harm. Lower courts have been inconsistent in observing tightly circumscribed boundaries for disclosure.[40] The Third Circuit's treatment of this issue is telling. Having found the broad informational interest to be "sufficiently important," the Third Circuit then deferred to the government's chosen means of compelling that disclosure.[41] The Ninth Circuit expressly ruled that a state's compelled disclosure scheme merely "furthers" the state's interest in "efficiency," even if the compulsory disclosure mechanism is unnecessary, overbroad, and harmful.[42]

The Court should set clear rules for the degree of tailoring between the government's asserted objective, if it justifies an infringement, and the compulsory exposure mechanism.

7. Are The Differences in Disclosure Mechanisms Constitutionally Significant?

Governments employ several common tools to expose political belief, speakers and associations. The primary tools are:

- Disclaimers – Speakers identify themselves on the face of a political communication. Sometimes the name of the immediate speaker is sufficient. Other times the government requires the speaker to identify itself as well as a designated number of the speaker's top donors or officers and directors. *McConnell* upheld disclaimers on the face of political ads that make use of the broadcast airwaves on the theory that the people own the airwaves and are entitled to know who is making a political use of them. *Talley* and *McIntyre* struck disclaimer requirements on pamphlets. *Buckley v. American Constitutional Law Foundation* struck name badges for petition circulators. Significantly, some disclaimer decisions analyze the mechanism under a forced speech doctrine

continued on page 22

Continued from page 21

rather than the compelled disclosure doctrine.[43]

- Communication-Specific Reports – Speakers must file a one-time report with a government agency identifying itself as the sponsor of a communication or other political activity. The invasiveness of the information demanded on the report can vary. One appeals court has upheld the FEC's rule requiring a one-time report filer to disclose only those funders who provided funds "for the purpose of" funding the communication that triggered the report.[44]
- Registration & Ongoing Reports – Speakers must file an initial registration and thereafter must file ongoing periodic reports disclosing varying details about their political activities. Political committee reporting at the FEC and lobbyist reporting under the Lobbying Disclosure Act are examples. Another example is the demand by some state attorneys general for nonprofit organizations to provide annually lists of all donors as a condition of soliciting contributions from citizens of their states.[45]
- Subpoena or Civil Investigative Demand – Speakers or associations are demanded to turn over internal materials about their political activities in connection with a government investigation or even civil litigation initiated by a political opponent. This tool of exposure was at issue in *Barsky*, *Lawson*, *Rumely*, *Sweezy*, *NAACP*, and a number of other cases.
- Investigative Hearing or Public Testimony – Government often demands disclosures in investigations and public testimony before legislative committees. It follows that if the government cannot require the disclosure legislatively, it cannot use the legislative fact-finding process to force the disclosure. The Court has ruled that the government cannot disclose by investigation that which is cannot disclose by legislation.[46]
- Submission of Political Records – Some political documents are necessarily submitted to the government in order to participate in the public election machinery. Voter registrations, for example, fit this category. In the ballot petition context, citizens sign petitions for the explicit purpose of submitting them to the government.
- Freedom of Information Disclosure or Similar Public Access – Sometimes the government holds private information about its citizens and discloses it to the public pursuant to freedom of information requests. This was the contested issue in *Doe v. Reed*, which upheld the public disclosure of petition signatures. But an appeals court blocked release of thousands of internal working records of the AFL-CIO under a provision of the FECA on the grounds that release would effect a severe First Amendment infringement.[47]

One would expect the Court to analyze closely the specific mechanism implemented by the government to determine if it actually advances the stated objective and whether another tool might be more effective and/or less invasive.

Moreover, assuming the Court confirms that disclosure is *per se* the constitutional harm, the degree of invasiveness should not be relevant to that part of the analysis. Instead, the degree of invasiveness – i.e., the breadth of the chosen disclosure mechanism – should be consider as part of the tailoring analysis. The frequency, detail, breadth, and burden of the disclosure mechanism should be considered here.

For example, retrospective investigative inquiries based upon articulated suspicion of specific wrongdoing should always be preferable to blanket, ongoing reporting. Specific law enforcement inquiries, such as subpoenas, guard against overbroad invasions of privacy and official mischief, they can be tested in a court for legitimacy,[48] and hold the government accountable to remain within its jurisdiction.[49] Mere expediency or government convenience to avoid the encumbrances of

continued on page 23

Continued from page 22

issuing subpoenas for information necessary to law enforcement should not override the First Amendment right.

Yet, increasingly systematic reporting requirements are replacing targeted subpoenas. Regular, systematic reporting mechanisms effectively operate like monthly or periodic subpoenas. Rather than receiving a case-specific subpoena for specific and necessary information, the citizen must provide the same information to the government but as a matter of regular course, subject to government prosecution or other punishment for failure to file a report. While the Court upheld regular reporting of campaign finances only for a narrowly defined category of "political committees" in *Buckley*, the Court has not approved regular, ongoing, detailed reporting of a charity's donors (having nothing to do with an election) or the expenditures by an organization that engages in issue advocacy, which lower courts increasingly are approving despite the overbreadth of the mechanism.[50]

Another important issue to be considered under this prong of the analysis should be the breadth of the audience chosen for exposure. Disclosure to government officials only (e.g., for law enforcement purposes) might be more narrowly tailored than exposure to the general public.[51] Yet courts have recognized the problem of official misuse of information by less than virtuous government officials.[52]

Some of the most significant disclosure mechanisms subject to legal confusion today are the rules triggering campaign finance disclosure. They include (1) the components of the "major purpose" test which triggers regulation of an organization as a "political committee" subject to extensive registration and ongoing reporting burdens and (2) expansion of the "electioneering communication" concept of federal law to force communication-specific exposure of broader realms of issue speech.[53]

The "major purpose" test, which is the subject of intensive litigation before federal courts today,[54] presents a fulcrum through which the Court could clarify many areas. "Political committees" must disclose all donors, all expenditures, and other sensitive information about their internal workings. For decades courts ruled that only the most explicit electoral activities over a long period of time could subject an organization to these invasive exposure burdens. More recently, a lower federal court decided about a half dozen other federal court rulings had been eclipsed by subsequent Supreme Court rulings[55] or were simply wrong, and ruled that wide swaths of issue advocacy can trigger full-blown disclosure of politically-oriented organizations.[56] By contrast, communication-specific disclosure is a more tailored mechanism for facilitating disclosure of some campaign expenditures. That too is the subject of ongoing litigation.

Finally, state requirements for issue-centric nonprofit organizations to submit their donor lists as a condition of soliciting donations is a hotly contested issue. All are these disclosure mechanisms are the subject of active legislative efforts, litigation, and shifting legal rationales. All are highly politicized topics. All suffer from the absence of definitive guidance from the Court.

8. Even if the Government Facially Justifies the Infringement, Can a Citizen Nevertheless Qualify for an Exception to Compulsory Exposure?

As summarized in Chapter 6, *Buckley* held that a facial uphold compulsory disclosure mechanism does not end the citizen's First Amendment protection. The citizen can still challenge the law's application to the citizen's unique circumstances. *Buckley* and *Doe v. Reed* recognize the relief valve of an *as-applied* challenge to an otherwise constitutional disclosure regime.

Buckley ruled that, even under a facially justifiable compulsory disclosure rule, a citizen can qualify for an exception to it by establishing a unique hardship using *NAACP* as a template. The citizen can prove up

continued on page 24

Continued from page 23

harassment, economic or other reprisals, threats of physical harm, or similar special circumstances that justify an exception to disclosure, that is, an exception to the exception. Similarly, *Doe v. Reed* addressed a facial challenge to Washington state's policy of making petition signatures available to the public. The Court went to lengths to limit its ruling to the facial challenge before it, reserving on any possible as-applied challenge. But the Court remanded the case for further fact-finding and analysis of the plaintiffs' as-applied challenge.

9. How Much Evidence of Harassment or Hardship Is Necessary?

When *Doe v. Reed* did return to the lower courts, the district court set an insurmountable evidentiary standard for the Doe plaintiffs, determined that the plaintiffs failed to justify an exception, and denied the plaintiffs' motion for a preliminary injunction.[57] Thereafter Washington state made the names of petition signers public, and the Ninth Circuit dismissed the appeal as moot.[58] Even the as-applied challenge was held to an elusive standard.

By contrast, a district court in California found that Americans for Prosperity Foundation did present sufficient evidence of harassment, reprisals, and threats to justify an as-applied injunction excepting it from turning over its donor lists. But the Ninth Circuit reversed.

The Ninth Circuit's implementation of the *Davis* language illuminates how some lower courts have diminished First Amendment protection by setting insurmountable evidentiary standards. The organization Americans for Prosperity Foundation, a non-electoral 501(c)(3) think tank, presented copious evidence that its founders and funders faced death threats, public vilification, economic retaliation in the form of boycotts, and enough harassment that its donor base was highly sensitive to exposure.[59] The trial court heard evidence and was convinced that state compelled exposure chilled the educational organization's donor base and harmed the associational rights of its members.[60]

On appeal, however, the Ninth Circuit imposed upon the Foundation a gauntlet of heightened evidentiary standards. The Ninth Circuit reasoned that although the Foundation's founders and funders were indeed subjected to death threats and harassment, the Foundation's lawyers could not specifically tie those threats to the Foundation's activities and, moreover, the Foundation could not specifically tie the associational chill to California's compulsory disclosure law.[61] Being controversial and facing threats in the political arena generally was not good enough, according to the Ninth Circuit.

Few organizations in America could meet that kind of evidentiary burden, even though they may be harmed nonetheless. It is difficult to prove up donors who chose not to associate due to concerns over a specific exposure law.

The Ninth Circuit's approach is far more burdensome than the Supreme Court has established for as-applied *exceptions* to compulsory disclosure in the campaign finance context. Even in that context, *Buckley* and *Brown v. Socialist Workers Party* set forth a less demanding evidentiary standard for citizens to justify an exception. *Buckley* "recognize[d] that unduly strict requirements of proof could impose a heavy burden" upon citizens associational chill, and therefore instructed lower courts to apply "sufficient flexibility in the proof of injury to assure a fair consideration of their claim."[62] The Court further instructed that "[t]he evidence offered need show only a reasonable probability that the compelled disclosure of a party's contributors' names will subject them to threats, harassment, or reprisals from either Government or private parties. The proof may include, for example, specific evidence of past or present harassment of members due to their associational ties, or of harassment directed against the organization itself. A pattern of threats or specific manifestations of public hostility may be sufficient. New parties that have no history upon which to draw may be able to offer evidence of reprisals and threats directed against individuals or organizations holding

continued on page 25

Continued from page 24

similar views."[63]

That this evidentiary standard was applied in *Buckley* and *Socialist Workers* to campaign finance disclosure, the north star of compelled public exposure regimes, indicates that no higher evidentiary standard should apply in other political speech and association contexts where the government can justify its forced exposure and a citizen or group seeks as-applied relief.

The Ninth Circuit's approach is likely far less protective of First Amendment rights than Justice Alito intended when he wrote *Davis*. Speaking of the evidentiary burden courts may impose upon citizens in *as-applied* challenges to exposure regimes that are ruled facially constitutional, Justice Alito wrote in *Doe v Reed* that "speakers must be able to obtain an as-applied exemption without clearing a high evidentiary hurdle. We acknowledged as much in *Buckley,* where we noted that 'unduly strict requirements of proof could impose a heavy burden' on speech."[64] Coming from the author of *Davis*, that articulation of the evidentiary standard should carry some weight.

Doe v. Reed confirmed that the *Buckley* procedure is not limited to minor political parties or vaguely defined "dissident" or "minority" points of view. Justice Alito articulated a general as-applied paradigm that was effectively followed by the plaintiffs who did not appear to constitute a distinctly "minor party" or "dissident" group. While the "dissident" nature of a viewpoint might be one factor that elicits a backlash, there are distinct costs to expressing even majority points of view, if indeed the courts could even classify all viewpoints into neat categories of majority, popular, minority, or "dissident" opinion. Surely First Amendment protection should not be conditioned on a poll of public opinion or subjective judicial judgments before affording equal protection to all Americans on a content-neutral basis. In the current distressed political environment particularly speakers of all perspectives can and do find themselves the subject of economic reprisals and boycotts, de-platforming protests, disinvitations, threats on the Internet, and any number of other severe responses to even the minutest of controversial remarks on all sides of the political spectrum.

Significantly, the Ninth Circuit has imposed upon citizens the heightened burden of establishing harassment and retaliation at the threshold of both facial and as-applied challenges. There is no escaping the heavy evidentiary burden of proving actual retaliatory acts and causally connecting them directly to a specific government disclosure law in the Ninth Circuit. The Ninth Circuit, perversely it seems, has set a much higher bar to qualify for any kind of constitutional scrutiny, shifting the high burden to the citizen at the front end of both facial and as-applied constitutional analyses.[65]

10. Avoiding Unnecessary First Amendment Conflicts Where Compulsory Disclosure Rules Are Extra-Statutory or Outside Agency Jurisdiction.

A reminder is in order that governmental interests are often delimited by statute or similar authorization. Therefore, before assessing a government's asserted interests under First Amendment scrutiny, a court should first satisfy itself that the compulsory disclosure is even within the agency's subject matter jurisdiction or authorized by statute. If it is not, then a court can reject the compulsory disclosure rule without further ado and avoid a First Amendment showdown. If there is ambiguity or doubt about the agency's subject matter jurisdiction, the court should interpret the agency's subject matter jurisdiction or statutory authorization narrowly to avoid the First Amendment question.

Courts have taken this approach in a number of cases. The four-Justice opinion of the Court in *Sweezy* determined that the New Hampshire Attorney General's inquiry into Paul Sweezy's fellow political travelers exceeded the scope of the Attorney General's authority under the relevant state statute. Courts have enjoined the FEC's attempt to investigate

continued on page 26

Continued from page 25

or disclose the internal secrets and activities of political organizations because the FEC was acting outside its statutory authority.[66]

Rumely invoked the doctrine of constitutional avoidance to narrowly construe the jurisdiction of the House Select Committee on Lobbying Activities (i.e., the "Buchanan Committee") and the definition of "lobbying" subject to disclosure. If a statute extends the government's asserted interest in compelling exposure far beyond a scope the First Amendment will bear, however, then a court should either strike the disclosure statute or save it by drawing the clear boundary to it. The Court did this in *Buckley*, imposing the "major purpose" limitation on "political committee" status and the "express advocacy" limitation on the realm of "expenditures" subject to regulation and disclosure.

In short, before entertaining a plaintiff's First Amendment challenge or a government agency's assertion of interest justifying a compulsory exposure rule, a court should first determine whether the compulsory exposure rule is even authorized by a clear government statute or policy. If there is doubt or ambiguity, the court should interpret the agency's jurisdiction narrowly and avoid the First Amendment problem. Only if that cannot be reasonably accomplished should the court jump into the First Amendment challenge.

Conclusion: Prospects at the Supreme Court

Predicting how the current Supreme Court would clarify the First Amendment right of political privacy is difficult. The pendulum has swung back and forth on the Court since the 1940s. There was a time when liberal Justices championed political privacy for communists, progressives, civil rights organizations, Jehovah's Witnesses, and even Margaret McIntyre as a paramount constitutional right while conservative Justices were most skeptical. Nevertheless, solid Court majorities eventually rendezvoused to protect political privacy.

But what has become of the once unanimous First Amendment right? Have the exceptions swallowed the right? Has the judicially-recognized exception for campaign finance disclosure overtaken all other realms of political activity disclosure? What kind of right is it if Congress, state legislatures, and state attorneys general wholly ignore it in legislation and investigations, usually targeted at their political or ideological opponents, while lower courts blithely write around it?

It is time for the Supreme Court to reset the proper judicial scrutiny and analysis for the important First Amendment right of privacy in political speech, association, and conscience. I will offer a few observations about the social cost of government's invasion of the political privacy of its citizens in the next, and last, chapter to this series.▪

For more information on the First Amendment Right to Political Privacy, please contact:

Lee E. Goodman
lgoodman@wileyrein.com
202.719.7378

continued on page 27

Continued from page 26

Endnotes

[1]*Sweezy v. New Hampshire*, 354 U.S. 234 (1957); *NAACP v. State of Alabama, ex rel. John Patterson*, 357 U.S. 449, 452 (1958); *Talley v. California*, 362 U.S. 60 (1960); *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995); *Watch Watchtower Bible and Tract Society of New York, Inc. v. Village of Stratton*, 536 U.S. 150 (2002).

[2]*See, e.g., Citizens United v. Schneiderman*, 882 F.3d 374, 383 (2nd Cir. 2018) ("requiring disclosure is not itself an evil"); *Center for Competitive Politics v. Harris*, 784 F.3d 1307, 1312-1314 (9th Cir. 2015) ("CCP is incorrect when it argues that the compelled disclosure *itself* constitutes such an injury, and when it suggests that we must weigh that injury when applying exacting scrutiny.").

[3]The Center for Competitive Politics has changed its name to The Institute for Free Speech. It is a non-profit organization under section 501(c)(3) of the Internal Revenue Code devoted to expanding free speech rights of all Americans and it engages in no electoral activity.

[4]*Center for Competitive Politics*, 784 F.3d at 1314.

[5]*See, e.g., Americans for Prosperity Foundation v. Becerra*, 903 F.3d 1000, 1009 (9th Cir. 2018) ("The mere possibility that *some* contributors *may* choose to withhold their support does not establish a substantial burden on First Amendment rights.").

[6]*Center for Individual Freedom, Inc. v. Tennant*, 706 F.3d 270 (4th Cir. 2013).

[7]*Citizens United v. Federal Election Commission*, 558 U.S. 310, 368-371 (2010); *McConnell v. Federal Election Commission*, 540 U.S. 93, 193 (2003).

[8]The Court has acknowledged the constitutional significance of the distinction between electoral speech and issue speech in a number of decisions. *See*, *Buckley v. American Constitutional Law Foundation*, 525 U.S. 182, 203 (1999) ("We note, furthermore, that ballot initiatives do not involve the risk of '*quid pro quo*' corruption present when money is paid to, or for, candidates."); *McIntyre*, 514 U.S. at 352 (same).

[9]*McConnell*, 540 U.S. at 193. The Federal Election Commission adopted a regulation limiting the donor disclosure to those donors who provided funds for the specific purpose of funding each electioneering communication, 11 C.F.R. § 104.20(c)(9), and the U.S. Court of Appeals for the District of Columbia Circuit upheld the regulation as an appropriate balance between donor exposure and the First Amendment right to political privacy. *Van Hollen v. Federal Election Commission*, 811 F.3d 486, 499 (D.C. Cir. 2016).

[10]*Delaware Strong Families v. Attorney General of Delaware*, 793 F.3d 304, 308 (3rd Cir. 2015) ("The Supreme Court has consistently held that disclosure requirements are not limited to 'express advocacy' and that there is not a 'rigid barrier between express advocacy and so-called issue advocacy.'") *citing McConnell*, 540 U.S. at 193; *Citizens United v. Federal Election Commission*, 558 U.S. 310, 368 (2010); *Wisconsin Right to Life*, 551 U.S. 449, 469-476 (2007).

[11]*Center for Competitive Politics v. Harris*, 784 F.3d 1307, 1312 (9th Cir. 2015); *Citizens United v. Schneiderman*, 882 F.3d 374, 382 (2nd Cir. 2018).

[12]*Doe v. Reed*, 130 S.Ct. 2811 (2010).

[13]*Americans for Prosperity Foundation v. Becerra*, 903 F.3d 1000, 1008 (9th Cir. 2018).

[14]*See, e.g., Citizens for Responsibility and Ethics in Washington v. Federal Election Commission*, 209 F.Supp.3d 77, 90 & n.8 (D.D.C. 2016); For the People Act of 2019 (H.R. 1, 116th Cong.); Maryland Online Electioneering Transparency and Accountability Act of 2018 (Md. Code Ann., Elec. Law § 13-405(c)); New York Executive Law §§ 172-e, 172-f (Chap. 286, Parts F, G).

[15]*Compare McConnell* (upholding FCC public file disclosure requirements for political messages communicated over broadcast airwaves, but leaving open as-applied challenges) *and Delaware Strong Families* (upholding Delaware law compelling disclosure of issue speech on the Internet) *and The Washington Post v. McManus*, 355 F.Supp.3d 272 (D.Md. 2019) (preliminarily enjoining Maryland FCC-like public file disclosure requirements for issue advertisements on the internet as applied to advertising platforms operated by press organizations).

[16]*See, e.g.*, *Americans for Prosperity Foundation*, 903 F.3d at 1012-1017.

[17]*Watchtower Bible*, 536 U.S. at 166 ("The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible."), *quoting McIntyre*, 514 U.S. at 341-342; *accord Talley*, 362 U.S. at 69 (Clark, *dissenting*); *Center for Individual Freedom*, 706 F.3d at 282.

[18]*Davis v. Federal Election Commission*, 554 U.S. 724, 745 (2008) (internal citations and quotations omitted).

[19]*DeGregory v. Attorney General of New Hampshire*, 383 U.S. 825, 829 (1966), *quoting Gibson v. Florida Legislative Investigation Committee*, 372 U.S. 539, 546 (1961).

[20]*Buckley*, 424 U.S. at 66, *citing NAACP v. Alabama*, 357 U.S. at 460-461.

[21]*Burson v. Freeman*, 504 U.S. 191, 198 (1992).

[22]*See, e.g., United States v. Hamilton*, 699 F.3d 356, 370 n.12 (4th Cir. 2012); *Pharm. Care Management Assoc. v. Rowe*, 429 F.3d 294, 309 (1st Cir. 2005); *Bernbeck v. Moore*, 126 F.3d 1114, 1116 (8th Cir. 1997); *Clark v. Library of Congress*, 750 F.2d 89, 94 (D.C. Cir. 1984); *Familias Unidas v. Briscoe*, 619 F.2d 391 (5th Cir. 1980).

[23]*See, e.g., Real Truth About Abortion, Inc. v. Federal Election Commission*, 681 F.3d 544, 549 (4th Cir. 2010); *Green Party of Connecticut v. Garfield*, 616 F.3d 213, 229 n.9 (2d Cir. 2010); *Vermont Right to Life Committee, Inc. v. Sorrell*, 758 F.3d 118, 133 n.12 (2d Cir. 2014); *Alaska Right to Life Committee v. Miles*, 441 F.3d 773, 787 (9th Cir. 2006).

[24]*See, e.g., Libertarian Party of Ohio v. Husted*, 751 F.3d 403, 413 (6th Cir. 2014); *Minnesota Citizens Concerned for Life, Inc. v. Swanson*, 692 F.3d 864, 876 (8th Cir. 2012); *Schneiderman*, 882 F.3d at 382; *Americans for Prosperity Foundation*, 903 F.3d at 1009; *Center for Competitive Politics*, 784 F.3d at 1312-1314.

[25]*Delaware Strong Families*, 793 F.3d at 310.

[26]*Schneiderman*, 882 F.3d at 382.

continued on page 28

Continued from page 27

[27]*Doe v. Reed*, 561 U.S. at 232 (Thomas, *dissenting*).

[28]*Delaware Strong Families v. Denn*, 136 S.Ct. 2376, 2378 (2016) (Thomas *dissenting* from the denial of certiorari). Justice Alito also voted to grant certiorari, but did not join Justice Thomas' written rationale. Since that time, Justices Gorsuch and Kavanaugh have joined the Court raising speculation about whether there might be four Justices to grant certiorari in a future disclosure case.

[29]*United States v. Playboy Entertainment Group, Inc.*, 529 U.S. 803, 812-813 (2000) (applying "strict scrutiny" to content-based speech regulations); *McIntyre*, 514 U.S. at 357 (holding that a ban on political speech because it omits government-compelled information is a content-based speech restriction).

[30]*The Washington Post v. McManus*, 355 F.Supp.3d 272, 289-290 & n. 14 (D. Md. 2019).31

[32]*Buckley*, 424 U.S.at 64-68.

[32]*Citizens United*, 558 U.S. at 366-367.

[33]*Americans for Prosperity*, 903 F.3d at 1011 (approving state's "important" interest), at 1014 (characterizing necessary burden on associational rights as "substantial"), at 1019 (upholding compelled disclosure of non-profit's organization's donors "[b] ecause the burden on the First Amendment right to association is modest, and the Attorney General's interest in enforcing its laws is important").

[34]*See, Americans for Prosperity Foundation*, 903 F.3d at 1009-1012; *Schneiderman*, 882 F.3d at 382-384.

[35]*Americans for Prosperity Foundation*, 903 F.3d at 1010 ("the state's quick access to Schedule B filings increases the Attorney General's investigative efficiency") (internal quotations and citations omitted).

[36]As the D.C. Circuit recently phrased the problem, the elevation of transparency policy "treats speech, a constitutional right, and transparency, an extra-constitutional value, as equivalents." *Van Hollen*, 811 F.3d at 501.

[37]*McIntyre*, 514 U.S. at 347.

[38]*NAACP v. Button*, 371 U.S. 415, 438 (1963); *Buckley*, 424 U.S. at 41.

[39]*See, e.g., Center for Individual Freedom*, 706 F.3d at 282.

[40]*Compare Van Hollen* (upholding FEC's "for the purpose of" donor disclosure rule with respect to electioneering communications) *with Citizens for Responsibility and Ethics in Washington v. Federal Election Commission*, 316 F. Supp. 3d 349 (D.D.C. 2018) (striking FEC's decades-old "for the purpose of" donor disclosure rule with respect to independent expenditures).

[41]*Delaware Strong Families*, 793 F.3d at 310.

[42]*Americans for Prosperity Foundation*, 903 F.3d at 1011.

[43]*See, e.g., McIntyre*, 514 U.S. at 348; *The Washington Post*, 355 F.Supp.3d at 286.

[44]*Van Hollen*, 811 F.3d at 498-499.

[45]*See, e.g., Center for Competitive Politics*; *Americans for Prosperity Foundation*; *Schneiderman.*

[46]*DeGregory v. Attorney General of New Hampshire*, 383 U.S. 825, 829 (1966) ("Investigation is a part of lawmaking and the First Amendment, as well as the Fifth, stands as a barrier to state intrusion of privacy.").

[47]*AFL-CIO v. Federal Election Commission*, 333 F.3d 168, 177-179 (D.C. Cir. 2003).

[48]*DeGregory*, 383 U.S. at 829-830 (quashing subpoena to testify about citizen's past political activities); *Watkins v. United States*, 354 U.S. 178, 197-200 (1957) (same); *United States v. Rumely*, 345 U.S. 41, 46-48 (1953).

[49]*See Federal Election Commission v. Machinists Non-Partisan Political League*, 655 F.2d 380, 387-388 (quashing FEC subpoena that intruded upon the privacy of political activities outside the agency's jurisdiction); *United States v. National Committee For Impeachment*, 469 F.2d 1135 (2nd Cir. 1972) (ruling government could not force an organization to register and file reports disclosing its finances because the organization's activities were outside government's disclosure jurisdiction).

[50]*See, e.g.*, *Americans for Prosperity Foundation*, 903 F.3d at 1010 (government's law enforcement "efficiency" overrides wholly lawful charity's right to donor privacy); *Citizens for Responsibility and Ethics in Washington ("CREW I") v. Federal Election Commission*, 209 F.Supp.3d 77, 92 (D. D.C. 2016) ("[T]he majority of circuits have concluded that ... disclosure requirements [related to registration and reporting] are not unduly burdensome.") (internal quotation and citation omitted).

[51]This issue has figured centrally in several court rulings. *See, e.g., Doe v. Reed* (ruling that disclosure to the general public enhanced the government's objective of confirming the validity of petition signatures); *Buckley v. American Constitutional Law Foundation* (ruling that certain disclosures, such as the identities of petition circulators, were permissible to the government but overbroad and counterproductive when made to the public); *Center for Competitive Politics v. Harris* (upholding forced disclosure because donor lists would be seen only by government officials, not the general public); *Americans for Prosperity v. Becerra* (same).

[52]*Schneiderman*, 882 F.3d at 383 ("Law enforcement officials have been known to abuse their power, and there is always a risk that an office charged with care of confidential information will spring a leak. A list of names in the hands of those with access to a state's coercive resources conjures up an uneasy number of troubling precedents.").

[53]*See, e.g., Delaware Strong Families* (expanding reporting to internet postings and direct mail); *Center for Individual Rights* (expanding reporting to messages published in print media).

[54]*See, Citizens for Ethics and Responsibility in Washington ("CREW") v. Federal Election Commission*, Case No. 16-2255 (D. D.C.) (pending); *Public Citizen v. Federal Election Commission*, Case No. 14-00148 (D. D.C.) (pending).

[55]*Citizens for Ethics and Responsibility in Washington (CREW I) v. Federal Election Commission*, 209 F.Supp.3dd 77, 91-92 (D. D.C. 2016). The district court in *CREW* reasoned that *McConnell* had opened the door to disclosure of "electioneering communications," a form of issue advocacy, that *Citizens United* had endorsed disclosure, and therefore the funding

continued on page 29

Continued from page 28

of electioneering communications subjected an organization to full-blown registration and reporting burdens as a "political committee." *See also, Citizens for Ethics and Responsibility in Washington (CREW II) v. Federal Election Commission*, 299 F.Supp.3d 83 (D. D.C. 2018).

[56] *CREW,* 209 F.Supp.3d at 91-92 & n. 8.

[57] *Doe v. Reed*, 823 F.Supp.2d 1195, 1201 (W.D. Wash. 2011) ("For an as-applied challenge to a law such as the (Washington Public Records Act] to succeed, there would have to be a *significant threat* of harassment directed at those who sign the petition *that cannot be mitigated by law enforcement measures*…. I would demand strong evidence before concluding that an indirect and speculative chain of events imposes a substantial burden on speech…. The as-applied exemption that Doe seeks has been upheld in only a few cases," such as NAACP and Socialist Workers Party).

[58] *Doe v. Reed*, 697 F.3d 1235 (9th Cir. 2012).

[59] *See* Complaint for Preliminary and Permanent Injunctive Relief and for a Declaratory Judgment (Dec. 9, 2014), *Americans for Prosperity Foundation v. Harris*, Civil Action No. 2:14-cv-09448 (U.S.D.C. C.D. Cal.).

[60] *Americans for Prosperity Foundation v. Harris*, 182 F.Supp.3d 1049 (C.D. Cal. 2016).

[61] *Americans for Prosperity Foundation*, 903 F.3d at 1015-1017.

[62] *Buckley*, 424 U.S. at 74; *Brown v. Socialist Workers Party*, 459 U.S. 87 (1982).

[63] *Id.*

[64] *Doe v. Reed*, 561 U.S. 186, 204 (Alito, *concurring*).

[65] *See Center for Competitive Politics*, 784 F.3d at 1314 (facial challenge); *Americans for Prosperity Foundation*, 903 F.3d at 1012-1014 (as-applied challenge).

[66] *See, e.g.*, *Federal Election Commission v. Machinists Non-Partisan Political League*, 655 F.2d 380, 389 (D.C. Cir. 1981) ("[I] f … the FEC lacks jurisdiction to enforce contribution limitations on 'draft' groups, then no compelling interest for the subpoenaed information can possibly exist. The highly sensitive character of the information sought simply makes it all the more important that the court be convinced that jurisdiction exists to conduct this investigation before it enforces subpoenas issued pursuant thereto.").

Privacy and Cybersecurity at Wiley Rein

Rachel A. Alexander	202.719.7371	ralexander@wileyrein.com
Megan L. Brown	202.719. 7579	mbrown@wileyrein.com
Jon W. Burd	202.719.7172	jburd@wileyrein.com
Bethany A. Corbin	202.719.4418	bcorbin@wileyrein.com
Scott D. Delacourt	202.719.7549	sdelacourt@wileyrein.com
Matthew J. Gardner	202.719.4108	mgardner@wileyrein.com
Boyd Garriott	202.719.4487	bgarriott@wileyrein.com
Lee E. Goodman	202.719.7378	lgoodman@wileyrein.com
Peter S. Hyun*	202.719.4499	phyun@wileyrein.com
Bruce L. McDonald	202.719.7014	bmcdonald@wileyrein.com
Dorthula H. Powell-Woodson	202.719.7150	dpowell-woodson@wileyrein.com
Duane C. Pozza	202.719.4533	dpozza@wileyrein.com
Kathleen E. Scott	202.719.7577	kscott@wileyrein.com
Joan Stewart	202.719.7438	jstewart@wileyrein.com

**Not admitted to the District of Columbia Bar. Supervised by principals of the firm who are members of the District of Columbia Bar.*