Wiley Rein LLP

# PRIVACY IN FOCUS®

**Developments in Privacy and Information Security Law** | March 2019

2019 has been a busy year for privacy and cybersecurity, much as we anticipated at the start of the year. From Congress to the states to the courts to agencies such as the Federal Trade Commission – where I worked until joining Wiley Rein last year – privacy debates have been front and center. This month we bring you not only a full slate of articles, but a month-long series of webinars on cutting-edge privacy topics featuring attorneys across our Privacy, Cyber & Data Governance Practice.

In this issue, Megan Brown, Joan Stewart, Kat Scott, law clerk Boyd Garriott, and I recap February's privacy-related developments, including two key congressional hearings and NIST's release of its Privacy Framework Working Outline. Joan Stewart and Kat Scott dig deeper into the California Consumer Privacy Act and discuss practical steps to come into compliance. Lee Goodman discusses a recent court decision – now on appeal – enjoining a Maryland statute requiring certain disclosures in political ads. Megan Brown, Scott Delacourt, Matt Gardner, Kat Scott, and I discuss the FTC's proposed changes to its cybersecurity rules for financial institutions, issued by a 3-2 vote. And Lee Goodman provides the latest installment of his series analyzing First Amendment political privacy rights.

In addition, below are links to our March Privacy & Cybersecurity Webinar Series, including links where you can listen to any webinars you may have missed.

Our talented group of privacy and cybersecurity attorneys has a wide range of expertise that they will continue to share in these pages and I'm happy to edit *Privacy in Focus* at such an eventful time. 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. Our contact information is listed on each article. Thank you as always for reading.

***—Duane Pozza, Partner, Privacy, Cyber & Data Governance Practice***

## ALSO IN THIS ISSUE



## February Was a Big Month in Privacy: Here's What You Need to Know

**By Megan L. Brown, Duane C. Pozza, Joan Stewart, Kathleen E. Scott, and Boyd Garriott***

February was a busy month in privacy – from the federal government to the states, from legislatures to agencies, various governmental authorities have been hard at work on a diverse array of potential privacy approaches. Here is a quick overview of the action and some key takeaways:

### U.S. Congress

*House of Representatives*

On February 26, the House Subcommittee on Consumer Protection and Commerce of the Committee on Energy and Commerce held its first hearing of the 116th

*continued on page 2*

*continued from page 1*

Congress to discuss the merits of federal data privacy legislation.

On the surface, there were two broad bipartisan themes: (1) concern over how businesses use consumer data; and (2) support for a federal privacy bill. But despite this principal overlap, there was considerable breakdown on partisan lines. Republicans were generally more concerned with creating a single, federal standard, and also raised the risk that overly prescriptive regulations would adversely affect small businesses. Democrats were more concerned with creating enforceable consumer rights and reducing the burden on consumers to navigate complex privacy policies.

*Senate*

On February 27, the Senate Committee on Commerce, Science, and Transportation held its own hearing on privacy policy principles.

This hearing signaled bipartisan consensus that it is time for comprehensive federal privacy legislation and that the Federal Trade Commission (FTC) should be its primary enforcer. However, there were still notable partisan divisions. The split over preemption was more obvious than in the House, with Chairman Roger Wicker (R-MS) explicitly endorsing preemption and Ranking Member Maria Cantwell (D-WA) suggesting that preemption may be unnecessary. Additionally, Democrats generally inquired about specific privacy protections, whereas Republicans tended to focus on broad transparency principles.

## NIST

The National Institute of Standards and Technology (NIST) is also focusing on privacy and is working to draft a Privacy Framework. On February 27, NIST released an analysis of the nearly 80 responses it received responding to its November request for information (RFI). And on the same day, NIST also released a Privacy Framework Working Outline – addressing some of the comments from the RFI responses – "for discussion purposes to promote input on the NIST Privacy Framework: An Enterprise Risk Management Tool."

In the analysis of the RFI responses, NIST noted that there was broad support for its development of the framework. Additionally, NIST found that commenters generally favored, *inter alia:*

- Regulatory compatibility: "the Framework should support organizations' ability to comply with a large range of legal responsibilities, including U.S. state and federal sector-specific laws and regulations and international regimes ...";
- The basic NIST Framework attributes, including "common and accessible language, that it be adaptable, risk-based, outcome-based, technology-agnostic, non-prescriptive, and readily usable as part of an enterprise's broader risk management processes ..."; and
- Inclusivity of emerging technologies, such as Internet of Things (IoT) and artificial intelligence.

In the Privacy Framework Working Outline, NIST explains that the Privacy Framework will, at a high level, be aligned with the Cybersecurity Framework. It will provide a "Privacy Framework Core" made up of functions, categories, subcategories, and informative references that will "present key privacy outcomes identified by stakeholders as helpful in managing privacy risk." The functions – which organize high-level data

*continued on page 3*

privacy activities related to data processing – are (1) identify; (2) protect; (3) control; (4) inform; and (5) respond.

The Outline also discusses the "Privacy Framework Profile," which is the "alignment of [the Privacy Framework Core] with the business requirements, risk tolerance, privacy objectives, and resources of the organization" and four "Privacy Framework Implementation Tiers," that "provide context on how an organization views privacy risk and the processes in place to manage that risk." The Profile and Tiers are intended to allow for risk management and flexibility, by helping an organization identify which functions, categories, and subcategories of the Privacy Framework are appropriate for its organizational needs.

NIST is hosting a series of workshops on the development of this Framework, with the next workshop scheduled for May 13-14 in Atlanta.

## NTIA

On February 26, David J. Redl, the Assistant Secretary of Commerce for Communications and Information, gave remarks on privacy at the Mobile World Congress Ministerial Programme. In it, he outlined the National Telecommunications and Information Administration's (NTIA) thinking on privacy.

Broadly speaking, Secretary Redl noted the desire to create global interoperability but stressed that his goal was to create "a fundamentally American approach to privacy, built on the same bedrock principles that so many nations share." He also stressed "a sense of urgency and a desire for American leadership" on privacy.

In terms of specifics, he supported a preemptive, risk- and outcome-based approach, stating that:

- There is broad industry consensus on both domestic and global interoperability and correspondingly opposition to "a patchwork regulatory landscape within the U.S."
- "[F]ocusing on risks and outcomes is preferred to notice-and-consent approaches." He argued that a risk- and outcome-based focus was best because it does not create a check-the-box mindset or entrench large businesses at the expense of startups and small firms.

Lastly, he argued that privacy is bound up with cybersecurity, saying "you cannot have true privacy without secure network technology. We're ready to work together to ensure that our technology infrastructure is secure."

## FTC

Also in February, the FTC rescheduled its privacy hearing, which had been postponed due to the government shutdown earlier this year. The hearing – which is part of the FTC's larger series of hearings on Competition and Consumer Protection in the 21st Century – is now scheduled for April 9-10. Explaining that its current and long-standing approach to privacy "needs to be examined in light of potential gaps in the Commission's existing authority, as well as new risks, new opportunities, and new knowledge," the FTC has posed a series of questions for public input, including:

- What are the actual and potential benefits for consumers and to competition of information collection, sharing, aggregation, and use? To what extent do consumers today, or are consumers likely to, realize these benefits?

*continued on page 4*

*continued from page 3*

- What are the actual and potential risks for consumers and to competition of information collection, sharing, aggregation, and use? To what extent do consumers today, or are consumers likely to, realize these risks?
- Should privacy protections depend on the sensitivity of data? If so, what data is sensitive and why? What data is not sensitive and why not?
- Should privacy protection depend on, or allow for, consumer variation in privacy preferences? Why or why not? What are the appropriate tradeoffs to consider? If desired, how should this flexibility be implemented?
- What are existing and emerging legal frameworks for privacy protection? What are the benefits and drawbacks of each framework?
- What are the tradeoffs between ex ante regulatory and ex post enforcement approaches to privacy protection?

Comments will be due on May 31.

### California Consumer Privacy Act

On February 20, the California State Assembly held a legislative hearing on the California Consumer Privacy Act (CCPA). Many at the hearing raised concerns about the law, largely centered around the short turnaround for implementation, the potential negative economic impact of the law, and how the private right of action should function.

Relatedly, several bills have been introduced in California to amend or clarify the CCPA, including California Senator Hannah-Beth Jackson's SB 561 that is supported by the California Attorney General and would expand the law's private right of action, among other changes.

Lastly, the California Attorney General is in the preliminary stages of a rulemaking to create "procedures to facilitate consumers' rights under the CCPA and ... guidance to businesses for how to comply."

Comments were due March 8. ■

For additional information on these and other emerging regulatory trends, please contact:

**Megan L. Brown**
202.719.7579
mbrown@wileyrein.com

**Duane C. Pozza**
202.719.4533
dpozza@wileyrein.com

**Joan Stewart**
202.719.7438
jstewart@wileyrein.com

**Kathleen E. Scott**
202.719.7577
kscott@wileyrein.com

**Boyd Garriott***
202.719.4487
bgarriott@wileyrein.com

**Wiley Rein Law Clerk Boyd Garriott contributed to this article.*

# California Consumer Privacy Act: Steps You Can Take Now to be Prepared

**By Joan Stewart and Kat Scott**

The California Consumer Privacy Act (CCPA) takes effect January 1, 2020 (although AG enforcement will be delayed until July 1, 2020, or until six months after the implementing regulations are published – whichever comes first). While the law is still subject to change – the state legislature is considering various amendments to the current law and the Attorney General is just wrapping up the preliminary stages of the rulemaking process to develop implementing regulations – your business can and should start compliance efforts now.

The CCPA applies to a for-profit business that collects a California resident's personal information, does business in California, and meets at least one of the following criteria: (1) has annual gross revenues in excess of $25 million; (2) receives or discloses the personal information of 50,000 or more consumers, households or devices per year; or (3) derives 50% or more of their annual revenues from selling the personal information of California residents. There are limited exceptions to the scope of the law, including for information that is governed by the HIPAA or the Gramm-Leach-Bliley Act.

While on initial glance, you may think your company does not "**collect**" "**personal information**" or "**sell**" that information, dig a little deeper because these definitions are broad.

- Collecting personal information includes: "buying, renting, gathering, obtaining, receiving, or accessing any personal information."
- Personal Information is even more broadly defined to include traditional information such as name and address, as well as audio, electronic, visual, thermal, and olfactory information; commercial records (personal property, products, services purchased); biometric information; unique personal identifiers (IP addresses, cookies, beacons, etc.); internet information, such as browsing history and search history; geolocation information; professional or work information; and inferences drawn from any of that information to create a profile of the consumer. Basically, if you can directly or indirectly connect it to a natural person who is a California resident, it is likely personal information.
- Finally, you may not think that you sell personal information, but the CCPA defines "sell" to include, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating (orally, in writing, electronically, or by other means) a consumer's personal information for monetary or other valuable consideration.

If you still don't think the CCPA applies to you, then you have made a lucky escape; for everyone else, keep reading.

The CCPA requires that you clearly communicate with consumers about what personal information you are gathering, what you are doing with it, who you are sharing it with, and that they have certain rights to their data. This information can all be communicated in your business's privacy policy. Be sure to update your policy every 12-months – that's also a CCPA requirement. The CCPA gives consumers certain rights to their personal information – including,

*continued on page 6*

*continued from page 6*

among other things, the right to know what personal information you have collected about them during the past 12 months (the right to access) and the right to request that you delete it. If you are selling their data (remember the broad definition), then they also have the right to "opt-out" of that sale. Or, if they are a minor, you must have their guardian "opt-in" to the sale.

The CCPA is still subject to change, and the California legislature is currently considering multiple proposed amendments. Additionally, the state Attorney General is charged with drafting implementing regulations. The Attorney General just received comments following the preliminary stages of the rulemaking and expects to issue draft regulations by this Fall with final regulations on schedule for early next year (perhaps).

Even with this uncertainty as to the final law and how it will be implemented, there are important steps your company can take now to prepare for the CCPA.

- **Know your data.** Take this opportunity to audit your data and create a data map. What data are you collecting, what purpose are you collecting it for, who are you sharing it with?
- **Review your privacy policy.** Does it accurately reflect what data you are collecting and what you are doing with that data? Does it clearly communicate who you are sharing the data with and for what purpose?
- **Don't leave your service providers and vendors out of the review process.** Review your agreements with any third party. Make sure you understand how data is flowing between you and your vendors, and that your agreement reflects what data is being shared and for what purpose.
- **Start investigating how you can comply with the obligations to track and honor the various consumer rights.** Could you quickly and accurately respond to an opt-out request or a request for deletion? What systems do you need in place to be able to do this?

While it is tempting to put off thinking about the CCPA until there is more clarity, no company that will be subject to its requirements has that luxury. It is important to start preparing now. ■

For more information on the CCPA and related compliance challenges, please contact:

**Joan Stewart**
202.719.7438
jstewart@wileyrein.com

**Kathleen E. Scott**
202.719.7577
kscott@wileyrein.com

# Federal Court Enjoins Maryland Internet Disclosure Law, But...

**By Lee E. Goodman**

A U.S. District Court has preliminarily enjoined enforcement of the Maryland Online Electioneering Transparency and Accountability Act as likely violating the First Amendment. As viewed by Judge Paul W. Grimm, the statute, enacted in May 2018, was Maryland's legislative response "to revelations that Russia exploited social media in a campaign to sway public opinion in the United States ahead of the 2016 presidential election." The act requires social media and press websites that carry online advertising to collect information about the sponsors of political ads and to publish that information for state and public inspection. It would impose burdens on websites such as *The Washington Post, The New York Times*, Facebook, Twitter, and similar websites that sell online advertising space.

*The Washington Post* and other news organizations brought suit challenging the statute in August, leading to the subject January preliminary injunction ruling. *The Washington Post v. McManus*, 2019 WL 112639 (D. Md.). The state has now appealed the preliminary injunction to the Fourth Circuit, where briefing is scheduled to begin in April. (T*he Washington Post v. David J. McManus, Jr.*, No. 19-1132). Consequently, this test of First Amendment rights merits continuing attention.

## Judge Grimm's Analysis

"All compelled disclosure laws implicate the Free Speech Clause," the court wrote, "but laws imposing those burdens on the media implicate a separate First Amendment right as well: the freedom of the press." After noting the lack of clarity in case law over whether disclosure requirements in the campaign finance area trigger "strict scrutiny" or "exacting scrutiny," the court applied "strict scrutiny," where the government bears the burden of showing the challenged regulation "furthers a compelling interest and is narrowly tailored to achieve that interest."

In doing so, Judge Grimm rejected Maryland's argument that a less demanding "exacting scrutiny" standard applies, under which Maryland contended the government must demonstrate merely that disclosure requirements are "substantially related" to an "important" government interest. Maryland argued that the more lenient standard was held applicable to campaign finance law disclosure requirements in *Buckley v. Valeo*, 424 U.S. 1 (1976), a characterization of *Buckley* that some commentators dispute. Judge Grimm observed the exacting scrutiny standard was upheld as to requirements imposed directly on "candidates, campaigns, political committees or donors." Because the Maryland statute imposed disclosure obligations on independent third-party press entities, applying exacting scrutiny here would go beyond the exception to strict scrutiny established by *Buckley*. He declined to expand the exception.

The court ruled the Maryland law did not meet the "strict scrutiny" test for restrictions upon First Amendment rights of the press, because it forces them to collect and post publicly information that they, in their editorial judgment, otherwise would choose not to publish, in violation of legal precedents proscribing such government dictates on the press. The court also ruled that Maryland could obtain the same information by imposing legal responsibilities directly upon

*continued on page 8*

*continued from page 7*

ad sponsors rather than the neutral third-party web platforms.

In analyzing the statute under the strict scrutiny test, Judge Grimm accepted that "states have a compelling interest in preventing foreign governments and their nationals from interfering in their elections." The problem was that the Maryland statute appeared not "'narrowly tailored' to promote these interests, meaning that 'no less restrictive alternative would serve its purposes.'" A statute fails if it is "overinclusive" so that it "unnecessarily circumscribes protected expression" or "underinclusive" and thus "leaves appreciable damage to the government's interest unprohibited." The court found that the statute failed because it "regulates substantially more speech than it needs to while, at the same time, neglecting to regulate the primary tools that foreign operatives exploited to pernicious effect in the 2016 election."

Overinclusiveness included that the statute imposed publication, record-keeping, and government access requirements on all "online platforms," defined so broadly as to sweep in many entities, not just "social media giants," even though "the state has not been able to identify so much as a single foreign-sourced paid political ad that ran on a news site, be it in 2016 or at any other time."

Underinclusiveness included that the statute applied only to paid political ads whereas the "primary evil the act was intended to redress was *unpaid* Internet postings (many of which mentioned no election or candidate at all)." Thus, the statute would not really address the problem.

Judge Grimm then went on to find that even if a less demanding "exacting scrutiny" standard applied, the Maryland statute would fail due to the "mismatch" of the disclosure requirement's "means and its ends." Here the requirements "are duplicative of other campaign finance disclosure requirements," "they do not target the deceptive practices that Act ostensibly seeks to deter," and "they are poorly calibrated to prevent foreign operatives from evading detection."

The court stopped short of enjoining the law altogether, choosing instead to enjoin its application to the specific press plaintiffs who brought the challenge (*The Washington Post, Baltimore Sun*, Capital-Gazette Communications LLC, APG Media of Chesapeake LLC, Community Newspaper Holdings Inc., Ogden Newspapers of Maryland LLC, Schurz Communications Inc., and the Maryland-Delaware-D.C. Press Association, Inc.).

## Broader Implications

The Fourth Circuit appeal presumably will involve numerous arguments about what standards should apply to the First Amendment review of statutes that impose burdens on Internet platforms and require disclosure of the identity of payors. The January preliminary injunction decision undercuts the conventional wisdom that disclosure statutes are always constitutional when they touch candidate elections. If the district court ruling stands, it should impact the behavior both of legislatures and administrative agencies, some of which have been working to expand compelled disclosure requirements.

The implications are important for current legislative efforts like the Honest Ads Act in the last Congress and other state laws

*continued on page 9*

*continued from page 8*

that attempt to regulate Internet-based advertising platforms. In several respects, the Maryland law is less onerous than the burdens proposed for web and press platforms in the Honest Ads Act (which would impose both civil and criminal liability). Judge Grimm's decision will likely introduce caution in Congress, especially if it is upheld by the Fourth Circuit.

The decision also has implications for potential efforts by agencies such as the Federal Election Commission (FEC) to impose legal responsibility and liability upon advertising platforms for the posting of disclaimers. The issue arose in a matter resolved by the FEC in early 2018 involving a political ad run in the *Chesterland News*, an Ohio newspaper (Matter Under Review 7210). For over 35 years, the FEC has imposed legal responsibility for ad disclaimers solely upon ad sponsors, who control funding and content of the ads, not advertising platforms. Yet, last year, two of the six Commissioners proposed to alter that long-standing rule in the *Chesterland News* matter. The effort failed. The issue was analyzed in a Concurring Statement of Commissioner Lee E. Goodman dated February 12, 2018, which discussed the First Amendment rights of the press to resist such liability: **http://eqs.fec.gov/eqsdocsMUR/18044436380.pdf**. Decisions like Judge Grimm's would inhibit such attempts in the future. ■

For additional information on rights protected by the First Amendment, please contact:

**Lee E. Goodman**
202.719.7378
lgoodman@wileyrein.com

# FTC Announces Proposed Changes to Cybersecurity Regulation for Financial Institutions

**By Megan L. Brown, Scott D. Delacourt, Matthew J. Gardner, Duane C. Pozza, and Kathleen E. Scott**

On March 5, the Federal Trade Commission (FTC) announced proposed revisions to its Safeguards Rule, which governs data security practices for financial institutions under the FTC's Gramm-Leach-Bliley (GLB) Act jurisdiction. The proposed revisions – which were issued by a 3-2 vote – would expand the scope of companies covered by the Rule and mandate that covered entities take certain specific steps to secure customers' information, including encryption and multifactor authentication. This proposal marks a distinct shift in the FTC's approach to data security for financial institutions. The proposed revisions opt for a top-down, regulatory approach akin to the New York Department of Financial Services' (DFS) cybersecurity regulation, which also mandates certain data security practices, including encryption and multifactor authentication. As the two dissenting Republican Commissioners describe it, "[t]he current proposal ... trades flexibility for a more prescriptive approach."

The FTC's Safeguards Rule requires covered financial institutions to develop, implement, and maintain a comprehensive information security program containing safeguards to collect and handle customer information. The safeguards must be reasonably designed to ensure the security and confidentiality of customer information, protect against any anticipated security threats, and protect against unauthorized access or use that could result in substantial harm or inconvenience. The safeguards must be appropriate to the size and complexity of the company, the nature and scope of its activities, and the sensitivity of the customer data.

## Proposed Additions

The proposed amendments, in the Commission's view, "continue to provide companies with flexibility, [but] also attempt to provide more detailed guidance as to what an appropriate information security program entails."[1] And the Commission cited, with approval, previous industry comments suggesting that non-bank financial technology companies – fintechs – should be subject to rules akin to those applicable to banks under Federal Financial Institutions Examination Council (FFIEC) Interagency Guidelines. The proposed requirements include:

- Developing a cybersecurity incident response plan;
- Designating a single individual to coordinate the company's information security program;
- Basing the information security program on a risk assessment and periodically performing additional risk assessments;
- Placing access control on information systems to authenticate users and permit access only to authorized individuals;
- Identifying and managing data, personnel, devices, systems, and facilities;

*continued on page 11*

[1] Notice of Proposed Rulemaking (NPRM) at 5.

*continued from page 10*

- Restricting access to physical locations containing customer information only to authorized individuals;
- Encrypting all customer information, both in transit and at rest;
- Adopting secure development practices for in-house developed applications for transmitting, accessing, or storing customer information;
- Implementing multifactor authentication for any individual accessing customer information or internal networks that contain customer information;
- Including audit trails designed to detect and respond to security events;
- Developing procedures for the secure disposal of customer information no longer necessary for business operations or other legitimate business purposes;
- Adopting procedures for change management, which govern the addition, removal, or modification of elements of an information system;
- Implementing policy and procedures to monitor the activities of unauthorized users and detect unauthorized access to customer information;
- Implementing training and education policies to enact the information security program;
- Monitoring service providers to assess the adequacy of their safeguards on an ongoing basis;
- Requiring the chief information security officer to provide certain annual reports about information security to the company's Board of Directors.

In the Notice of Proposed Rulemaking (NPRM), the FTC also seeks comment on whether financial institutions should be required to report security events to the Commission, and whether a Board should be required to certify compliance with the Rule. It also proposes to exempt institutions with relatively small amounts of customer information from certain parts of the Rule.

## More Companies Covered

Additionally, the proposed amendments would expand the scope of "financial institutions" covered under the rule to include companies significantly engaging in activities "incidental to financial activities." And in particular, the definition would include companies acting as "finders"– with "finding" defined as bringing together buyers and sellers of products or services for transactions that the buyers and sellers themselves negotiate and consummate. The Commission suggested that these companies should be subject to safeguard requirements because "they collect, maintain, and store sensitive consumer information ... [and] [i]f this sensitive information were to get into the wrong hands, consumers could suffer identity theft, fraud, or other harms."[2]

*continued on page 12*

[2] NPRM at 19.

## *FTC Announces Proposed Changes to Cybersecurity Regulation for Financial Institutions*

*continued from page 11*

Notably, Commissioners Noah Phillips and Christine Wilson dissented from the NPRM, arguing that the proposed regulations may not be appropriate for all market participants, are premature to enact, and conflict with the existing flexible approach to data security – imposing costs without clear consumer benefits. They also criticize the proposals for substituting the Commission's own judgment for private companies' governance decisions.

Additionally, in a separate NPRM, the Commission is seeking comment on proposed revisions to its Privacy Rule under the GLB Act. Unlike the vote on the Safeguards Rule NPRM, the vote on the Privacy Rule proposal was 5-0.

For both NPRMs, comments will be due 60 days after publication in the Federal Register. ■

For more information on the GLB proposals, please contact:

**Megan L. Brown**
202.719.7519
mbrown@wileyrein.com

**Scott D. Delacourt**
202.719.7459
sdelacourt@wileyrein.com

**Matthew J. Gardner**
202.719.4108
mgardner@wileyrein.com

**Duane C. Pozza**
202.719.4533
dpozza@wileyrein.com

**Kathleen E. Scott**
202.719.7577
kscott@wileyrein.com

# *Chapter 6 —The First Amendment Right to Political Privacy*

## Campaign Finance and Other Very Public Exceptions to Privacy

**By Lee E. Goodman**

### Introduction – The Right and Its Exceptions

Previous chapters have traced the origin and development since the 1940s of the First Amendment right to privacy in the political sphere. That right manifested as the right to associate, speak, and access information for political purposes free from government compelled exposure.

Over the same period of time, the U.S. Supreme Court was grappling with discrete realms of government-compelled exposure and carving exceptions to the constitutional protection. The exceptions were drawn narrowly upon the Court's findings that "substantial" government objectives outweighed the constitutional right under one form or another of constitutional scrutiny. The most prominent exceptions were compelled disclosure of financial contributions to direct lobbying of members of Congress and contributions to candidates' campaigns. This chapter summarizes the jurisprudence of exceptions to the right of political privacy.

### The Lobbyist Disclosure Exception (1950s)

Beginning with the Buchanan Committee's[1] inquisition of Edward Rumely's Committee for Constitutional Government (CCG) in 1951, the Supreme Court recognized that Congress' authority to demand disclosure of those who provide funding to support "lobbying" activities runs into First Amendment protections. To avoid the conflict, the Court interpreted the term "lobbying activities" narrowly to authorize Congress to require disclosure of CCG funders only in connection with CCG's "representations made directly to the Congress, its members, or its committees." [2] But Congress would run into the "prohibition of the First Amendment" if it attempted to exercise "power to inquire into all efforts of private individuals to influence public opinion through books and periodicals, however remote the radiation of influence which they may exert upon the ultimate legislative process."[3]

A year later, the Court was presented with a direct First Amendment challenge to lobbyist registration and funder disclosure mandated by the Federal Regulation of Lobbying Act. In *United States v. Harriss*,[4] the Court restricted the realm of disclosure, citing *Rumely*, to direct communications with members of Congress that were funded with that "principal purpose" as the object of the funding.[5]

In fact, the Court performed so much narrowing surgery to the scope of "lobbying" subject to mandated disclosure that Justices Douglas and Black, in loyal dissent, chastised the majority for rewriting the statute to save it from First Amendment infirmity. "The difficulty is that the Act has to be rewritten and words actually added and subtracted to produce the [constitutional] result," wrote the dissent.[6]

The extent of statutory narrowing to save the statute is one indication of how narrow the court conceived the exception to privacy in the realm of issue advocacy in *Harriss*.

*continued on page 14*

*continued from page 13*

Indeed, 40 years later, in *McIntyre v. Ohio*,[7] the modern Court characterized *Harriss* as "limited disclosure requirements for lobbyists" justified only because lobbyists "have direct access to elected representatives," which "if undisclosed, may well present the appearance of corruption."[8] And the exception to political privacy was limited in scope to *compensated* communications to directly influence elected officials.

Although the Court, in 1954, had yet to develop a formula of First Amendment scrutiny to justify what it acknowledged to be a First Amendment infringement, it nonetheless resorted to an analysis similar to modern day strict scrutiny. The Court found that the First Amendment restriction "is designed to safeguard a vital national interest" (analogous to a compelling governmental interest).[9] The Court also observed that the disclosure rule informed members of Congress "who is being hired, who is putting up the money, and how much" when they are lobbied so that they could act in the public interest (i.e., narrowly tailored to advance the government's objective). And finally, the Court observed that the disclosure measure did not prohibit lobbying (i.e., a least restrictive means).[10]

### The Campaign Finance Disclosure Exception (1970s)

The *Harriss* Court analogized the disclosure of lobbyist financing to the kind of donor disclosure required of political campaign committees under the Federal Corrupt Practices Act, a law in place since 1925, which, in the Court's judgment, "maintain[ed] the integrity of a basic governmental process."[11] Implicit in the comparison was the view that Congress could infringe the right to privacy where money was spent either to lobby or elect politicians.

In the first decade of the 20th century, a handful of states enacted laws requiring campaigns for public office to disclose the identity of their donors.[12] Disclosure and the issue of corporate contributions also were being debated in Congress, leading up to the passage, in 1907, of a law prohibiting corporate contributions and amendments in 1911 and 1925 (the Federal Corrupt Practices Act) to require campaigns and national parties to disclose donors and expenditures.[13]

In 1934, the Supreme Court had occasion to consider the constitutionality of the Federal Corrupt Practices Act. Although the political story underlying the Court's decision is too long to explain here, it suffices to summarize as follows. A prominent Methodist cleric, Virginia Democrat, and leader in the American temperance movement, Bishop James Cannon, had led a successful political revolt against Virginia's segregationist "Byrd Machine" in the 1928 presidential election, delivering Virginia to Republican Herbert Hoover against Democrat Alfred Smith who opposed Prohibition. For that apostasy the good Bishop had to endure a five-year retaliatory campaign led by Virginia's Democratic Senator Carter Glass, whose political vendetta spurred investigations and trials by national church tribunals, two committees of the U.S. Senate, and the U.S. Department of Justice, and an indictment and trial in federal court. Bishop Cannon was ultimately exonerated in all tribunals, but, as intended, was forever ruined as a cleric and political leader.[14]

*continued on page 15*

## Chapter 6 —The First Amendment Right to Political Privacy
### *Campaign Finance and Other Very Public Exceptions to Privacy*
*continued from page 14*

During the course of defending his federal indictment for failing to properly disclose a loan and disposition of the funds in connection with the 1928 presidential campaign in Virginia, Bishop Cannon and his assistant, Ada Burroughs, challenged the Federal Corrupt Practices Act under Article 2, Section 1 of the Constitution, which provides that each state has the authority to appoint its presidential electors as it sees fit. The argument was that requiring presidential campaigns to disclose their donors and disbursements infringed the state's sovereignty in choosing presidential electors. The Court disagreed, however, finding that the law did not "interfere with the power of a state to appoint electors or the manner in which their appointment shall be made."[15] Furthermore, the Court observed, the law was within Congress' authority "to preserve the purity" of presidential elections.[16]

Although the decision came decades before the Court recognized the First Amendment right to anonymity in the political sphere, its reasoning nonetheless recognized the governmental interest at stake. Like *Harriss*, the Court sustained the law under an analysis that resembled the modern strict scrutiny doctrine. The Court recognized the "importance" and "vital" interest in safeguarding the country from "the improper use of money to influence" election results and "insidious corruption."[17] The Court then foreshadowed the future test for narrow tailoring focusing on whether "the means adopted are really calculated to attain the end, the degree of their necessity, the extent to which they conduce to the end, the closeness of the relationship between the means adopted, and the end to be attained."[18] The Court accepted Congress' "conclusion that public disclosure of political contributions, together with the names of contributors and other details, would tend to prevent the corrupt use of money to affect elections. The verity of this conclusion reasonably cannot be denied."[19] The Court concluded that "it seems plain that the statute as a whole is calculated to discourage the making and use of contributions for purposes of corruption."[20]

The Court's recognition, in 1934, of the relationship between campaign money, corruption, and disclosure would go on to form the bedrock of campaign finance jurisprudence for the next century. The next major Court decision addressing the issue came in 1976, passing on the constitutionality of sweeping post-Watergate campaign finance reforms codified in the 1974 amendments to the Federal Election Campaign Act of 1971 (FECA), in the seminal case of *Buckley v. Valeo*.[21]

In *Buckley*, the Court was asked to declare FECA's donor disclosure regime unconstitutional, this time under the First Amendment right to privacy of conscience that had developed in the 1950s.[22] The Court first acknowledged that FECA's disclosure mandates infringe free speech and associational rights under *NAACP* and its progeny. "[W]e have repeatedly found that compelled disclosure, in itself, can seriously infringe on privacy of association and belief guaranteed by the First Amendment," the Court began.[23] The Court further recognized that once the government compels exposure, it is responsible for all repercussions visited upon the political organizations, even from private criticism.[24] And the Court ruled "the invasion of privacy of belief may be as great

*continued on page 16*

*continued from page 15*

when the information sought concerns the giving and spending of money as when it concerns the joining of organizations."[25]

The Court ruled that such severe infringements "cannot be justified by a mere showing of some legitimate governmental interest," rather, "the subordinating interests of the State must survive exacting scrutiny" and the information subject to compelled disclosure must bear a "substantial relation" to the government's valid interests.[26] The Court referred to this as the "strict test established by *NAACP v. Alabama*."[27]

Applying this "strict test," the Court found that FECA's disclosure requirements "directly serve substantial governmental interests."[28] Citing *Burroughs*, the Court decided that the prevention of corruption is a "substantial governmental interest" that justifies compelled exposure of direct campaign contributors as well as independent spenders who fund communications expressly advocating the election or defeat of federal candidates.[29] Disclosure of a candidate's direct campaign donors, the Court found, informs voters of the interests to which politicians might be most responsive or beholden.[30]

In the ensuing 40 years, the Court has continued to uphold disclosure of money spent with the direct effect of electing candidates. First, in 2010, the Court reaffirmed *Buckley*'s approval of compelled disclosure of independent expenditures expressly advocating the election or defeat of candidates in *Citizens United v. FEC*.[31] Second, the Court expanded constitutional tolerance for compelled disclosure of those who pay to run issue ads that merely reference candidates over broadcast media on the eve of candidate elections ("electioneering communications") in the 2003 decision *McConnell v. FEC*.[32]

### Exception to the Exception

Although *Buckley* found the government's interests substantial enough to justify the First Amendment infringement in general, it nevertheless limited disclosure in certain contexts. Too much disclosure, the Court recognized, could be a bad thing. First, the Court limited disclosure to spending on a narrow realm of direct election influencing, such as contributions to candidates and express advocacy ads. Second, the Court established a special exception from disclosure for small or unpopular political organizations especially vulnerable to harassment, threats, or reprisals in accordance with *NAACP*.[33] The Court thus established an exception to the exception to accommodate the most severe consequences of disclosure.

A few years later, in 1982, the Court returned to privacy under this exception in *Brown v. Socialist Workers '74 Campaign Committee*, which applied *Buckley*'s exception from compelled exposure for a minor political party.[34]

### The Public Petition Drive Exception (2008)

Two of the Court's more significant disclosure decisions in recent years were *Doe v. Reed*[35] and *Buckley v. American Constitutional Law Foundation, Inc*.[36] The subject of both cases was citizen participation in state-sponsored petition drives and ballot question elections.

In *Doe v. Reed*, the Court reviewed Washington state's direct democracy procedure by which 4% of the state's registered voters could by petition place

*continued on page 17*

*continued from page 16*

legislative questions on a statewide ballot. The petitions were signed and submitted to the state and checked for accuracy. Washington State considered the petitions to be public records subject to public availability under the state's public records law. Certain petitioners did not question the need to disclose their signatures, names and addresses to the state as part of the petitioning process, but they challenged release of the petitions to the public as a violation of their First Amendment right to political privacy. The Court held that the activity at issue was an inherently public act of signing a petition as a quasi-legislative act. Accordingly, the Court sustained release of the petitions to the public under a facial challenge to the law in this context.

Indeed, it is impossible to imagine how a state might require the signatures of 4% of all registered voters without expecting the signatures to be provided to the government and checked for validity.[37] In this way the activity in *Doe v. Reed* was like voting, where each voter must appear before a clerk, state her name and address and exhibit a form of identification, with party observers watching, to maintain the integrity of the election.

In *Buckley v. American Constitutional Law Foundation, Inc.*, the Court upheld compelled disclosure of the people who *fund* petition drives in Colorado, but the Court struck compelled disclosure of the names and addresses of petition circulators.

The upshot of the two decisions is that those who fund and sign petitions to invoke the state-sponsored ballot machinery engage in sufficiently public acts, in a sufficiently public election procedure, that their names can be disclosed publicly. But the Court drew the line there, finding that those who merely pass clip boards to obtain signatures are protected by the First Amendment, confirming that there is a boundary to compelled exposure.

### Do These Petition Drive Exceptions Affect Issue Speech Generally?

*Doe v. Reed* has become a favorite reference point for advocates of greater exposure of political participants generally, even in the issue speech arena, and even beyond the context of ballot petitions. Others see it as a highly contextual ruling, standing for the unremarkable proposition that participation in a state-operated ballot petition process is an inherently public act over which the state has responsibility for implementing with integrity.

Although rationales given in seven different opinions[38] did little to clarify this area of jurisprudence, a couple of points did appear clear. First, eight Justices (except Scalia) recognized that disclosure constitutes an infringement on First Amendment rights. However, at least four Justices (Sotomayor, Stevens, Ginsberg, Scalia) thought there was little infringement given the inherently public nature of the legislative act at issue. Second, eight Justices (except Thomas) were impressed by the state's responsibility to conduct a fair and honest election process and were willing to accept some degree of disclosure to advance that objective. Third, at least two Justices (Alito, Breyer) thought an as-applied challenge was an appropriate relief valve to the facially acceptable infringement.

The cacophony of concurring and one dissenting opinions makes it difficult to discern clear jurisprudence beyond the context of the public petition procedure at issue. Four Justices (Sotomayor, Stevens,

*continued on page 18*

*continued from page 17*

Ginsburg, Scalia) acknowledged that signing the petitions was essentially a public legislative act, substantively and legally different from private speech and associational activities.[39] Justice Scalia, who never believed there is a constitutional right to speak or associate privately, went so far as to argue that the act of voting historically was a public act and there is no constitutional right to vote secretly.[40]

On the other side of the spectrum is *McIntyre*, which ruled the government cannot force a pamphleteer advocating the defeat of a ballot referendum to identify herself in her literature. Of course, Ms. McIntyre was not a formal cog in the state's official election machinery. She did not fund a petition drive. She did not circulate government-issued petitions. She did not sign a petition. After a policy question was placed on a public ballot, Ms. McIntyre advocated the defeat of the question. Her speech was pure issue speech, not electoral advocacy on behalf of an impressionable politician. And it was her private activity, not an exercise of state-sponsored election machinery. For that purely private issue speech, the state had little grounds for compulsory exposure other than official voyeurism. The Court drew a line there.

Significantly, the Court has on several occasions distinguished between the acceptable levels of regulation in the two realms of advocacy – candidate speech versus issue speech.[41] The former is corruptible; the latter is not. This distinction may be the key to understanding a bright line in privacy jurisprudence – that money spent directly to influence politicians is the tipping factor justifying an exception to political anonymity and privacy. And taking that distinction one step further, one might distinguish privately funded issue speech from political activity that is a formal implementation of a state-run election apparatus.

In short, preventing corruption (i.e., *quid pro quo* arrangements with politicians) justifies compelled exposure of spenders in candidate elections, while election integrity justifies exposure of those who invoke the official state machinery of initiative and referenda elections. But private issue speech, even advocacy about a ballot question, arguably remains a private domain. It is a domain, however, that remains under constant inquisition as well as legislative and regulatory efforts to compel its disclosure too.

### Two Lines of Law – Privacy Versus Its Exceptions

In summary, the Court has developed two lines of precedents in tension with each other. One steadfastly protects the right to privacy in the political sphere, including the right of conscience, of speech, of access to information, and association, and even the right to vote a secret ballot. The other, summarized above, upholds exceptions to the right. The gray area that lies between the two lines has invited a seemingly boundless range of state legislative efforts and court challenges to FEC rules seeking to expand disclosure to ever broader realms of political speech – from express advocacy exhorting voters to vote for a candidate to benign or merely factual candidate references, to broader time periods before elections, to communications over other discreet media including print and the Internet, to a broader range of government purposes, and, most profoundly, to issue speech generally that

*continued on page 19*

*continued from page 18*

has no correlation to any candidate election, lobbying effort, or issue election apparatus. Nobody is sure where to draw the boundary line.

Although this series has focused almost exclusively on the Supreme Court's jurisprudence in an effort to trace the First Amendment right and illuminate its contours, there are hundreds of lower federal and state court opinions that, unfortunately, wander through the two lines seemingly picking and choosing the best privacy decision or exception to support its conclusion.

Contradictions between the two lines have been most acute in a handful of areas. First is the subject of ballot petitions and referenda campaigns outlined above. One interesting discussion of the lack of clarity in this speech realm has been detailed by Matt Miller of the Goldwater Institute. [42] Mr. Miller highlights conflicting circuit court opinions over the government's asserted "informational interest" to justify compelled exposure of donors to groups that speak about issues. Mr. Miller points to the Tenth Circuit as the circuit providing the most robust constitutional protection for privacy in the referenda speech realm. He cites two decisions, *Coalition for Secular Government v. Williams*[43] and *Sampson v. Buescher*.[44]

Second is the similar but distinct area of general issue speech. Here, Mr. Miller highlights doctrinal inconsistencies and conflicting results between the Tenth Circuit's protection for privacy in referenda campaigns and decisions upholding disclosure in the issue speech realm in the Third and Ninth Circuits.[45] Likewise, the First Circuit has ruled that issue speech is not subject to compelled disclosure.[46] Mr. Miller concludes, "The split in federal circuits about the ballot-initiative question is too deep for the Supreme Court to ignore forever. This is especially true since pro-disclosure laws are rapidly spreading across the country."

Third, an interesting issue has emerged in the Eighth Circuit over compelled registration and disclosure by individual citizens who lobby their representatives without compensation. The Eighth Circuit ruled that the disclosure rule of *Harriss* applied with equal force to the uncompensated discussions citizens have with their elected representatives.[47] That decision was a remarkable 2-to-1 decision with a very convincing dissent.[48] The Eighth Circuit has vacated the panel decision and has agreed to rehear the case *en banc*.

Fourth are government efforts, usually at the state level, to mandate nonprofit donor disclosure in the name of protecting consumers from fraudulent nonprofit solicitations. The Ninth and Second Circuits recently upheld donor disclosure mandates in the name of empowering state Attorneys General to vaguely police the *bona fides* of IRS-recognized and compliant nonprofit organizations.[49] In one of those cases, the group Americans for Prosperity presented such an overwhelming amount of evidence of death threats, harassment, name-calling, and general political hostility that it may well have exceeded the amount of evidence presented by the NAACP in its case against Alabama.[50] The district court found the evidence to satisfy an exception to the Attorney General's demand for donor lists.[51] But the Ninth Circuit, in one of the less compellingly articulated opinions in this area, wrote around the evidence and the district court's findings to reverse and uphold the compelled

*continued on page 20*

*continued from page 19*

exposure of the group's donors. The Ninth Circuit's decision exposes many of the gaps in clarity of the law that would benefit from Supreme Court guidance.

Fifth is the area of inquisition into the internal records and workings of political organizations. The D.C. Circuit has been most protective of the privacy of political organizations against gratuitous government inquiry.[52] The Ninth Circuit also has protected intrusions into the internal affairs of political organizations, albeit pursuant to a different analytical framework than the D.C. Circuit.[53] However, that clearly established law did not stop a large cadre of state Attorneys General from announcing a multi-state investigation into a national think tank's climate studies.[54]

Sixth is the thicket of litigation over the metes and bounds of campaign finance disclosure on the fringes of campaign contributions and express advocacy expenditures and in gray areas of hybrid political activities discussing issues and politicians. That issue is currently brewing in the federal courts in the District of Columbia over the issue of which nonprofit organizations must register as "political committees" (i.e., PACs) and disclose all of their donors and disbursements. *Buckley* held that only those organizations that have as their "major purpose" the election or defeat of federal candidates can be compelled to register and publicly disclose all donors and financial activity.[55] Since that time, several federal courts have narrowly applied the "major purpose" test to organizations that devote a majority of their efforts to expressly advocating the election or defeat of candidates.[56] However, a more recent decision by one federal district court determined that all of those opinions are no longer good law and, moreover, ruled that the historical distinction between disclosure of issue speakers versus election speakers no longer has legal significance under the First Amendment.[57]

The legal analysis set forth in that most recent district court decision would upend decades of First Amendment jurisprudence and underscores the need for the Supreme Court to bring clarity and uniformity to this area of First Amendment jurisprudence. Not only have outcomes differed, but the analytical paths leading to the results have varied widely. Accordingly, legal observers generally agree that clarity is needed throughout these areas, even if they disagree sharply on the direction that clarity should take. Some believe the Court needs to bolster the analytical importance of the threshold First Amendment right. Others point to confusion over the jurisprudential level of scrutiny as the key to resolving the two lines. Others believe the Court needs to demand greater discipline and seriousness in the ascertainment of purported governmental interests, pointing to superficial review that has become typical in "exacting scrutiny" reviews. Transparency for the sake of transparency is often perceived by proponents of stronger constitutional protection of privacy as a particularly weak justification for compelling disclosure, and it often presents under rationales such as the "right to know who is speaking" or the generic "informational interest."

Lower courts also have openly complained about the lack of clear guidance. One federal court recently noted the lack of a clear standard of scrutiny for laws that compel disclosure of political speech and, as between "exacting scrutiny" or "strict

*continued on page 21*

*continued from page 20*

scrutiny," chose strict scrutiny to review a state campaign finance disclosure rule.[58]

More broadly, as the U.S. Court of Appeals for the D.C. Circuit recently observed in a significant campaign finance decision, the Supreme Court has been content to avoid "an answer to the important constitutional questions bubbling beneath the surface":

> [T]he Supreme Court's campaign finance jurisprudence subsists, for now, on a fragile arrangement that treats speech, a constitutional right, and transparency, an extra-constitutional value, as equivalents. But "the centre cannot hold."[59]

In sum, the Supreme Court's nods to both privacy and disclosure while resisting a comprehensive reconciliation of the constitutional limit on compelled disclosure policies has left lower courts across America to wander through idiosyncratic standards with often conflicting results. A reconciliation between the two competing principles is needed. Ideas for how we might reconcile the two lines of jurisprudence will be the subject the next chapter in this series. ■

For additional information on the First Amendment rights of political privacy, please contact:

**Lee E. Goodman**
202.719.7378
lgoodman@wileyrein.com

## Endnotes

[1] The formal name of the congressional committee was the House Select Committee on Lobbying Activities.

[2] *United States v. Rumely*, 345 U.S. 41, 47 (1953).

[3] *Id.* at 46.

[4] *United States v. Harriss*, 347 U.S. 612 (1954).

[5] *Id.* at 619-620.

[6] *Id.* at 629 (Douglas, joined by Black, *dissenting*).

[7] *McIntyre v. Ohio*, 514 U.S. 334 (1995).

[8] *Id.* at 356 n. 20.

[9] *Id.* at 626.

[10] *Id.* at 625.

[11] *Id.* at 625.

[12] *See* Robert E. Mutch, *Campaigns, Congress, And Courts: The making of federal campaign finance laws* (Praeger Publishers 1988), at pp. 8-9.

[13] *Id.* at 1-22.

[14] *See* Michael S. Patterson, "The Fall of a Bishop: James Cannon, Jr. Versus Carter Glass 1909-1934," The *Journal of Southern History*, Vol. 39,

*continued on page 22*

*continued from page 21*

No. 4 (Nov. 1973), pp. 493-518; Virginius Dabney, *Dry Messiah: The Life of Bishop Cannon* (Knopf 1949), at pp. 277-291.

[15] *Burroughs v. United States*, 290 U.S. 534, 544 (1934).

[16] *Id.*

[17] *Id.* at 545-546.

[18] *Id.* at 548.

[19] *Id.*

[20] *Id.*

[21] *Buckley v. Valeo*, 424 U.S. 1 (1976).

[22] *See* Chapters 1-5 of this series tracing the evolution of the First Amendment right to political privacy.

[23] 424 U.S. at 64, *citing Gibson v. Florida Legislative Committee*, 372 U.S. 539 (1963); *NAACP v. Button*, 371 U.S. 415 (1963); *Shelton v. Tucker*, 364 U.S. 479 (1960); *Bates v. Little Rock*, 361 U.S. 516 (1960); *NAACP v. Alabama*, 357 U.S. 449 (1958).

[24] *Id.* at 65, citing *NAACP*, 357 U.S. at 461 (holding that government exposure policy is necessarily responsible for private harassment and economic reprisals facilitated by the exposure).

[25] *Id.* at 66.

[26] *Id.* at 64.

[27] *Id.* at 66.

[28] *Id.* at 68.

[29] *Id.* at 67-68.

[30] *Id.*

[31] *Citizens United v. Federal Election Commission*, 558 U.S. 310 (2010).

[32] *McConnell v. Federal Election Commission*, 540 U.S. 93 (2003).

[33] 424 U.S. at 73-74.

[34] *Brown v. Socialist Workers '74 Campaign Committee*, 459 U.S. 87, 91-93 (1982). Justice Alito provided a similar approach in his concurring opinion in *Doe v. Reed*, positing that the analysis starts with the First Amendment right and recognition of an infringement. Next, the government bears the burden of justifying the infringement. If the government carries its burden of justifying the infringement in a facial challenge, citizens then have an opportunity to persuade a court to carve an exception to the government's disclosure rule in an as-applied challenge. 130 S.Ct. 2811, 2822-2827 (2010) (Alito, *concurring*).

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

[36] *Buckley v. American Constitutional Law Foundation, Inc.*, 525 U.S. 182 (1999).

[37] The Court found that public access to the petitions advanced the state's interest in election integrity because private groups would double check the integrity of the election, a proposition that Justice Alito doubted. 130 S.Ct. at 2825-2827 (Alito *concurring*).

[38] The seven opinions of *Doe v. Reed*: (1) Chief Justice Roberts' opinion of the Court (joined by Kennedy, Ginsburg, Breyer, Alito, Sotomayor); (2) Breyer's concurring opinion; (3) Alito's concurring opinion; (4) Sotomayor's concurring opinion (joined by Stevens, Ginsburg); (5) Stevens' concurring opinion (joined by Breyer); (6) Scalia's opinion concurring in the judgment; (7) Thomas's dissenting opinion.

*continued on page 23*

*continued from page 22*

[39] *Id.* at 2828-2929 (Sotomayor *concurring*), 2833-2934 (Scalia *concurring*).

[40] *Id.* at 2833-2934 (Scalia *concurring*). In addition to distinguishing the Washington State petition process from other contexts of private political association and speech, Justice Scalia reiterated his dissenting argument in *McIntyre* that there is no right to private political activity – not even to cast a secret ballot. *Id.* He endorsed the "civic courage" necessary to vote by voice (ironically, in a case litigated under the pseudonym "Doe").

[41] 514 U.S. at 356; *First National Bank of Boston v. Bellotti,* 435 U.S. 765, 790 (1978) ("Referenda are held on issues, not candidates for public office. The risk of corruption perceived in cases involving candidate elections simply is not present in a popular vote on a public issue.") (internal citations omitted).

[42] *See* Matt Miller, "Privacy And The Right to Advocate: Remembering *NAACP v. Alabama* and its First Amendment Legacy on the 60th Anniversary of the Case" (The Goldwater Institute Jan. 17, 2018).

[43] *Coalition for Secular Government v. Williams,* 815 F.3d 1267, 1277 (10th Cir. 2016).

[44] *Sampson v. Buescher*, 625 F.3d 1247 (10th Cir. 2010).

[45] Mr. Miller cites two opinions upholding disclosure in the issue speech realm generally: *Delaware Strong Families v. Delaware*, 793 F.3d 304, 312-313 (3d Cir. 2015); *Americans for Prosperity Foundation v. Harris*, 809 F.3d 536 (9th Cir. 2015).

[46] *Vermont Right to Life Committee, Inc. v. Sorrell*, 221 F.3d 376, 386-387 (1st Cir. 2000).

[47] *Calzone v. Summers*, 909 F.3d 940 (8th Cir. 2018), Opinion vacated and rehearing en banc granted Jan. 28, 2019.
[48] *Id.* at 952-956 (Stras, J., *dissenting*).

[49] *Americans for Prosperity Foundation v. Becerra*, 903 F.3d 1000 (9th Cir. 2018); *Citizens United v. Eric Schneiderman*, 882 F.3d 374 (2d Cir. 2018).

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

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

[52] *See American Federation of Labor and Congress of Industrial Organizations v. Federal Election Commission*, 333 F.3d 168, 176-178 (D.C. Cir. 2003); *Federal Election Commission v. Machinists Non-Partisan Political League*, 655 F.2d 380, 388-389 (D.C. Cir. 1981).

[53] *Perry v. Schwarzenegger*, 591 F.3d 1147, 1159-1165 (9th Cir. 2010).

[54] *See* David Hasemyer, Sabrina Shankman, "Climate Fraud Investigation of Exxon Draws Attention of 17 Attorneys General," Inside Climate News (Mar. 30, 2016) (available at https://insideclimatenews.org/news/30032016/climate-change-fraud-investigation-exxon-eric-shneiderman-18-attorneys-general).

[55] 424 U.S. at 79.

[56] *See Wisconsin Right to Life v. Barland*, 751 F.3d 804 (7th Cir. 2014); *New Mexico Youth Organized v. Herrera*, 611 F.3d 669 (10th Cir. 2010); *North Carolina Right to Life v. Leake*, 525 F.3d 274 (4th Cir. 2008); *Colorado Right to Life Committee, Inc. v. Coffman*, 498 F.3d 1137 (10th Cir. 2007); *Federal Election Commission v. Malenick*, 310 F.Supp.2d 230 (D.D.C. 2004); *Federal Election Commission v. GOPAC, Inc.*, 917 F.Supp. 851 (D.D.C. 1996).

[57] *Citizens for Responsibility and Ethics in Washington v. Federal Election Commission*, 209 F.Supp.3d 77, 90 & n. 8 (D.D.C. 2016) ("In the wake of *Citizens United,* federal appellate courts have resoundingly concluded that WRTL II's constitutional division between express advocacy and issue speech is simply inapposite in the disclosure context.").

[58] *The Washington Post v. McManus*, 2019 WL 112639 *15 (D. Md. Jan. 3, 2019) ("[W]hen analyzing the constitutionality of a compelled disclosure law, *Buckley* is not the starting point. The 'exacting scrutiny' standard it propounded is, on the contrary, a limited exception to the general rule that compelled disclosure laws, like all content-based regulations, must overcome strict scrutiny.").

[59] *Van Hollen v. Federal Election Commission*, 811 F.3d 486, 501 (D.C. Cir. 2016).

# March Privacy & Cybersecurity Webinar Series

**Throughout March, Wiley Rein's privacy & security team has been hosting a series of timely updates on fast-moving legislative and regulatory developments affecting data governance, cyber risk management, incident response, privacy engineering, public policy, and more. Please feel free to listen in!**

## Federal Privacy Update: Congress, NIST & More.

**Click *here* to listen on demand.**

## California Consumer Privacy Act (CCPA) Briefing.

**Click *here* to listen on demand.**

## What to Watch: FTC Forecast for 2019.

**Register *here* to listen on March 19, 2019 @ 12PM (EDT).**

## Biometrics News.

**Register *here* to listen on March 26, 2019 @ 2PM (EDT).**

## Events & Speeches

### *Federal Privacy Update: Congress, NIST & More*
***Wiley Rein Webinars***
**Megan L. Brown, Speaker,**
**Duane C. Pozza, Speaker,**
**Kathleen E. Scott, Speaker**
**March 4, 2019**

### *Exploring Frameworks to Advance Consumer Privacy*
***South by Southwest (SXSW)***
**Megan L. Brown, Speaker**
**March 9, 2019 | Austin, TX**

### *California Consumer Privacy Act (CCPA) Briefing*
***Wiley Rein Webinars***
**Matthew J. Gardner, Speaker,**
**Kathleen E. Scott, Speaker,**
**Joan Stewart, Speaker**
**March 13, 2019**

### *What to Watch: FTC Forecast for 2019*
***Wiley Rein Webinars***
**Megan L. Brown, Speaker,**
**Scott D. Delacourt, Speaker,**
**Duane C. Pozza, Speaker**
**March 19, 2019**

### *Biometrics News*
***Wiley Rein Webinars***
**Duane C. Pozza, Speaker**
**Kathleen E. Scott, Speaker**
**March 26, 2019**

### *Is There Cybersecurity in IoT?*
***ABA IoT National Institute (4th Annual)***
**Megan L. Brown, Speaker**
**March 27-28, 2019 | Washington, DC**

### *Consumer Financial Protection Enforcement Under Trump*
***ABA Section of Antitrust Law***
**Duane C. Pozza, Speaker**
**March 28, 2019 | Washington, DC**

### *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**

# 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 |

**Boyd Garriott, a Law Clerk in Wiley Rein's Telecom, Media, and Technology practice, contributed to this newsletter.*

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