Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | May 2019

We're happy to announce that the 2019 edition of Chambers USA: America's Leading Lawyers for Business has recognized Wiley Rein's Privacy, Cyber & Data Governance Practice as a nationwide leader. Chambers cites the great breadth and depth of the firm's experience in matters that range from health care privacy to cybersecurity breaches to regulatory data governance requirements, and names Megan Brown as a Recognized Practitioner in the field.

This issue reflects just some of the wide range of privacy, cybersecurity, and data governance issues that we handle, and that are top of mind for lawmakers, regulators, and industry. Our new partner Kevin Rupy provides insights on a high-profile topic on which he has testified before Congress: how to address illegal robocalls. On the Executive branch side, Megan Brown, Michael Diakiwski, and I discuss NIST's request for information on standards for artificial intelligence (AI) – including those addressing privacy and data security – as it develops a federal plan for AI standards over the summer, and Moshe Broder discusses the new Executive Order on the government's cybersecurity workforce. Lee Goodman analyzes social costs of political disclosure requirements and the First Amendment. And we include a Spotlight interview with partner Peter Hyun on his practice and congressional and state interest in privacy enforcement.

As always, please reach out to any of us with questions, and let me know if you would like to see certain topics addressed in our newsletter. We had great interest in our recent privacy and cybersecurity webinars (now archived here) and our panel discussion on legislative and agency developments on privacy and cybersecurity, and there's much more to come.

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:

2019 Will Be a Pivotal Year for Robocalls

By Kevin Rupy

Illegal robocalls remain a high-profile issue for industry, regulators, and elected officials. Such calls have consistently topped the list of consumer complaints at both the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) for several years running. As industry moves aggressively to deploy caller ID authentication technologies (commonly referred to as SHAKEN/STIR), legislators at the federal and state levels are also advancing a broad range of legislative approaches to address the problem. With the 2020

continued on page 2

Kevin Rupy, Industry Leader in Telecom Legal and Policy Issues, Joins Wiley Rein

During March, **Kevin G. Rupy**, former Vice President of Law and Policy at the United States Telecom Association (USTelecom), joined the firm as a partner in the **Telecom, Media & Technology (TMT) Practice**. An industry leader in traditional and emerging communications legal and policy issues, Mr. Rupy serves as a "go-to" attorney on key challenges facing the TMT industry.

At USTelecom, where he served for more than 13 years, Mr. Rupy represented Fortune 500 companies in the wireline broadband marketplace. On behalf of the association, he worked closely with multiple government agencies, Congress, member companies, and industry contacts on issues ranging from common carrier regulation to the areas of robocalls, cybersecurity, and copyright safe harbors for ISPs. He also helped secure major reforms of the Federal Communications Commission's (FCC) pole attachment regulations.

Kevin can be reached at 202.719.4510 or krupy@wileyrein.com.

2019 Will Be a Pivotal Year for Robocalls

Continued from page 1

election cycle already underway, robocalls are proving to be a bipartisan, and potent, issue. Given this confluence of factors, 2019 is shaping up to be a pivotal moment in the years-long battle against illegal robocalls targeting consumers.

Distinguishing Between Legal Versus Illegal Robocalls – Why it Matters

As robocalls remain under intense scrutiny, it is crucial for policymakers and stakeholders to distinguish between legal and illegal robocalls. Unfortunately, the two categories are often conflated by stakeholders and the media, resulting in a distorted picture of the actual problem. Legal robocalls are permitted under the Telephone Consumer Protection Act (TCPA) and can include calls regarding school closings, prescription reminders, or public safety emergencies. Illegal robocalls involve fraudulent activities, such as calls purporting to be from the IRS threatening arrest, tech support scams, and phishing schemes.

Questionable Data on Robocalls is Informing Public Policy

Given the important distinction between legal and illegal robocalls, it is imperative for all stakeholders to accurately gauge the problem through analysis of factually correct data. Unfortunately, current data regarding robocalling trends and the effectiveness of industry abatement efforts are flawed. In fact, the FCC cautioned earlier this year that "reports about and data related to robocalls, without detailed analysis, can blur the lines between legal robocalls, both welcome and unwelcome, and illegal robocalls."

Absent consistent reporting and understanding of

continued on page 3

2019 Will Be a Pivotal Year for Robocalls

Continued from page 2

these distinct categories of robocalls, continuing misrepresentation of such data may be misinforming policy actions by government stakeholders. As just one example, the widely reported YouMail Robocall Index stated that 5.2 billion robocalls were made in March 2019. Closer examination of the data, however, reveals that fewer than half of these calls were "scams" (i.e., illegal), while more than half (approximately 2.8 billion) were entirely legal robocalls, such as legal telemarketing calls and important payment reminders. Nevertheless, multiple media reports focused on the 5.2 billion statistic, including stories in *The New York Times* and *The Washington Post*, and elected officials and regulators often point to the broader statistic as a basis for government intervention.

Robocalls Are a Highly Bipartisan Issue – and State and Federal Legislators Are Acting

Despite current political partisanship – and with the 2020 election cycle already underway – robocalls are a highly bipartisan, potent issue in state and federal legislatures. At the federal level, six separate bills (and a discussion draft) have been introduced in the House this year. State legislatures are also moving aggressively to address the robocall issue through various measures, some of which have been passed into law.

Federal Legislation Is Moving in Both Chambers of Congress

The leading bill in the House, H.R. 946, the "Stopping Bad Robocalls Act," was introduced by House Energy and Commerce Committee Chairman Frank Pallone (D-NJ) on February 4, 2019. Among other things, the bill would update the TCPA's autodialer definition, and would mandate the deployment of SHAKEN/STIR call authentication technologies by a date to be determined by the FCC. Other bills, such as H.R. 2355, the "ROBO Calls and Texts Act," and H.R. 2298, the "ROBOCOP Act," would mandate the deployment of call authentication technologies by voice providers. The "ROBOCOP Act" would also require companies to offer free robocall blocking services to all their voice customers, and would create a private right of action for consumers against telecom companies that fail to authenticate calls and/or provide free call blocking tools to consumers.

The principal bill in the Senate – the TRACED Act (S. 151) – passed out of the Senate Commerce Committee on a unanimous, bipartisan basis, and is targeted for passage through unanimous consent. Among other things, the bill requires the FCC to establish rules regarding the blocking of unauthenticated calls, and to consider rules related to the provisioning of phone numbers under the North American Numbering Plan. The bill also establishes a framework that could mandate the implementation of SHAKEN/STIR standards by voice providers within 18 months of passage. The TRACED Act enjoys strong support in the Senate and is targeted for passage by early summer. Depending on the outcome of the various bills in the House, it is possible that Congress could send some form of robocall legislation to the President's desk later this summer.

State Governments Also Are Considering and Passing Robocall Legislation

Concurrent with these federal efforts, several states also are moving aggressively with their own disparate measures to address robocalls. California, Hawaii, and Kansas have each introduced legislation this year addressing robocall and/or TCPA-related issues, and New York has introduced two separate bills. While the state bills generally address the illegal robocall problem, several seek to achieve this goal through increased regulatory obligations on voice providers. For example, two bills in the New York legislature (Senate Bill S3297A, and A675A) and Hawaii's bill (HB 797) would mandate call blocking by voice providers. The New York Senate bill would also require voice providers to offer free call blocking tools to customers. Notably, the bill's preamble references the "47.8 billion robocalls" purportedly made in 2018,

continued on page 4

2019 Will Be a Pivotal Year for Robocalls

Continued from page 3

without acknowledging that approximately half were legal.

A bill in the California legislature (SB 208) would also mandate deployment of call authentication technology by carriers by July 1, 2020. In addition to these bills being highly problematic for voice providers, the proliferation of state activity on illegal robocall issues should also be of concern to the FCC. Passage of these bills into law could introduce significant tension into efforts by the FCC to implement cohesive and uniform federal policies with respect to the deployment of call authentication technologies and mitigation of illegal robocalls.

The FCC Is Maintaining Pressure on Industry and Appears Willing to Act

Finally, the FCC remains intensely focused on the robocall issue. FCC Chairman Ajit Pai has repeatedly identified robocalls as his top consumer issue and continues to pressure industry stakeholders to deploy the SHAKEN/STIR call-authentication standards. In November, 2018, Chairman Pai sent 14 letters to facilities-based voice providers and "demanded" the adoption of the SHAKEN/STIR standards, and called for them to be launched "no later than" 2019. Earlier this year, he reaffirmed this stance while noting that if it appeared industry would not meet the deadline, "the FCC will have to consider regulatory intervention." Industry will be under intense scrutiny with respect to its deployment of the SHAKEN/STIR standards in the coming year, and the FCC under Chairman Pai appears more than willing to impose federal regulatory obligations on voice providers should suitable progress fail to be made.

The Challenge Ahead in 2019

Illegal robocalls will remain a high-profile issue in 2019. Facilities-based voice providers will be under the microscope from federal and state officials as they deploy call authentication technologies into their networks that many in government hope will stem the tide of illegal robocalls. Absent a major change in the current robocall narrative, however, lawmakers and regulators at the federal and state levels have already shown their willingness and ability to move forward with legislative and regulatory approaches to resolve this issue. ▪

For more information on robocall-related developments, please contact:

Kevin G. Rupy
202.719.4510 | krupy@wileyrein.com

NIST Is Seeking Input on Federal Standards on the Use of Artificial Intelligence

By Duane Pozza, Megan L. Brown, and Michael L. Diakiwski

On May 1, the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce published a **request for information** (RFI) on an anticipated plan for federal engagement on standards for artificial intelligence (AI). The agency is seeking input on topics that include the technical standards and guidance that are needed to establish "trustworthy" aspects of AI technologies, including "accuracy, transparency, security, privacy, and robustness." The agency will also be hosting a workshop on May 30 to obtain public input on AI standards.

NIST's development of a federal plan on standards and tools to support "reliable, robust and trustworthy" AI systems is a central component of the Administration's Executive Order on AI, and will provide an important framework for the federal approach to AI going forward. We discuss the Executive Order in greater detail **here**. The workshop and comment period provide a key opportunity for stakeholders to engage on how the U.S. government defines and begins to address potential AI regulatory issues, which include how data is used and managed, whether AI processes need to be "explainable," and how to address potential bias concerns. NIST's work will be influential both domestically and in setting a course on international engagement on AI standards.

Comments in response to the RFI must be filed by ***May 31, 2019***, and in-person **registration** for the workshop closes on May 23.

The RFI

NIST seeks information to help develop "[t]imely and fit-for-for purpose AI technical standards," which NIST believes will be crucial for building trust in AI technologies and achieving economies of scale. In general, NIST seeks to understand:

- The current status and plans regarding the availability, use, and development of AI technical standards and tools;
- Needs and challenges regarding the existence, availability, use, and development of AI standards and tools; and
- The current and potential future role of federal agencies regarding the development and use of AI technical standards and tools.

The RFI also provides a list of topics covering the "major areas" of inquiry, which include:

- The need for AI technical standards and the challenges in identifying and developing them;
- Whether AI standards should be sector-specific or there should be cross-sector AI standards;
- Technical standards and guidance that are needed to establish "trustworthy" aspects of AI technologies, including "accuracy, transparency, security, privacy, and robustness;"
- Opportunities for and challenges to U.S. leadership in AI standards development;
- Federal agencies' needs for AI standards and involvement and their current involvement in standards development; and
- Actions the federal government can take to help ensure that desired AI standards are incorporated into practice.

The Workshop

NIST has also scheduled a workshop for ***May 30*** to discuss its plan for federal engagement on AI standards. The workshop will include both panels and working sessions. Topics will include the importance of effective U.S. leadership on AI standards, what

continued on page 6

New Executive Order Targets America's Cybersecurity Workforce

By Moshe B. Broder

On May 2, 2019, the President issued an Executive Order on America's Cybersecurity Workforce, which follows several recent Executive branch and legislative actions intended to strengthen cybersecurity in both the public and private sectors. The Executive Order includes several directives aimed at incrementally advancing cybersecurity skills and expertise, and reflects the continued momentum of cybersecurity efforts in industry and government.

Workforce Strengthening

The Executive Order begins by reciting the often discussed challenges in the cybersecurity industry. Broadly speaking, while a robust and skilled workforce is essential to economic and national security, there is a severe shortage of skilled cybersecurity professionals. The federal government plays a unique and critical role in fostering the advancement of cybersecurity talent, and this Executive Order seeks to address the inadequate supply of qualified personnel. Notably, the Executive Order acknowledges that, as a matter of policy, it is critical to facilitate "seamless movement" of cybersecurity professionals between the public and private sectors.

To address these challenges, the Executive Order mandates that agencies implement several directives. First, the federal cybersecurity workforce will benefit from a rotational assignment program, which will enable knowledge transfer and skill advancement of cybersecurity personnel. The program will include detailing nominated employees from and between the U.S. Department of Homeland Security (DHS) and other federal agencies. Program participants must meet requirements established in the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework (NICE Framework), and will also receive peer mentoring.

Requirements and Awards

The NICE Framework will also play an increasingly prominent role in other contexts directly applicable to contractors and industry. For example, the

continued on page 7

NIST Is Seeking Input on Federal Standards on the Use of Artificial Intelligence

Continued from page 5

technical standards already exist, the needs of federal agencies, and how the federal government can best engage on AI standard-setting.

NIST expects to release an annotated outline after the workshop concludes. Under the Executive Order, the plan must be finalized by ***August 10*** of this year.

NIST's engagement plan will be one of the first substantive moves by the federal government to tackle potential regulatory issues surrounding AI. Much as with its approach to **cybersecurity**, NIST's approach to AI standards could significantly influence how these technologies are adopted and used. The workshop and RFI are important opportunities for stakeholders to engage prior to the August 10 deadline for the final plan. ▪

For additional information, please contact:

Duane C. Pozza
202.719.4533 | dpozza@wileyrein.com

Megan L. Brown
202.719.7579 | mbrown@wileyrein.com

Michael L. Diakiwski
202.719.4081 | mdiakiwski@wileyrein.com

New Executive Order Targets America's Cybersecurity Workforce

Continued from page 6

NICE Framework lexicon and taxonomy will be incorporated into knowledge and skill requirements for informational technology and cybersecurity services contracts, and agencies will report on whether contractor personnel have the necessary knowledge and skills to perform the contractual tasks in accordance with the NICE Framework. Similarly, agencies must encourage voluntary integration of the NICE Framework into existing education and workforce developments efforts undertaken by state, local, non-governmental, and private entities.

The federal government will implement other measures designed to develop skills and expertise of the cybersecurity workforce. Federal agencies will utilize cybersecurity aptitude assessments in order to identify and reskill current employees to perform cybersecurity work. Agencies will also re-examine existing awards and decorations for federal and military personnel and establish new awards as necessary to recognize outstanding performance. Finally, an annual cybersecurity competition will be developed for federal civilian employees with the goal of identifying, challenging, and rewarding the best cybersecurity talent. The Executive Order calls for the first competition to be held before the end of 2019.

Awareness and Assessment

The Executive Order also includes provisions directed at more broadly strengthening the nation's cybersecurity workforce. These high-level directives range from raising awareness of the workforce shortage, transforming the learning environment and educational curriculum, and establishing metrics for evaluating the effectiveness of workforce investments. Federal agencies are also tasked with reporting requirements with respect to the cybersecurity workforce supporting critical infrastructure and defense systems, including identifying skill gaps and recommending curricula for closing such gaps through training and other education.

This Executive Order follows the Administration's September 2018 National Cyber Strategy and Executive Order 13800, as well as the National Defense Authorization Act for Fiscal Year 2019 (NDAA), each of which featured multiple provisions highlighting the increasing role for industry and federal contractors in cybersecurity. Industry should expect to see continued Executive Branch action and legislation surrounding these issues. ▪

For additional information, please contact:

Moshe Broder
202.719.4186 | mbroder@wileyrein.com

Wiley Rein Spotlight Interview: Partner Peter Hyun on Congressional and State Approaches to Privacy

PIF: Tell us about your background prior to coming to Wiley Rein.

Peter: Before joining the firm 7.5 months ago, I was Chief Counsel to U.S. Senator Dianne Feinstein, where I advised her on a multitude of issues, including cybersecurity and tech issues as they related to law enforcement functions – such as Section 230 of the Communications Decency Act and the Stored Communications Act. By virtue of working for the Senator – who held senior positions on the Judiciary and Intelligence committees – I was able to get briefed on those topics by top government, public-sector, and private-sector folks. So I was quite spoiled and learned as much as I could. Before going to the Hill, I was a white collar civil fraud AUSA at the U.S. Attorney's office for the Eastern District of Virginia, and before that I was an Assistant Attorney General in the New York State Attorney General's office.

PIF: What actions have you seen states take on privacy issues?

Peter: Generally speaking, many states have been extremely active in policymaking and enforcing privacy laws. During the 2018 election, many incumbents and challengers in State AG races hammered the consistent message that they were going to prioritize enforcement of privacy violations and data breaches. And in fact, they have – with record-setting settlements reached in cases involving data breaches, violations of the Children's Online Privacy Protection Act (COPPA), and other privacy-related matters. These high-profile actions have put individuals and entities on notice that states are actively monitoring this space for compliance.

PIF: Congress has been looking at passing privacy legislation and also pushing agencies to investigate privacy issues more. What are the key Committees on these issues?

Peter: While the Senate Commerce and House Energy and Commerce Committees typically run point on data breach and other consumer issues, theoretically, nearly every other Committee in Congress can make an argument for why privacy issues are squarely within their jurisdiction – whether it's the Judiciary Committee, Intelligence Committee, Homeland Security Committee, etc. The fact is, getting privacy legislation accomplished in Congress will require broad buy-in from a multitude of committees, and not just one.

PIF: Do you think we'll see Congress investigate data privacy and security issues directly?

Peter: Absolutely. The investigative power of Congress is premised upon its Article I legislative power – and with policymakers grappling right now with how to write federal privacy legislation, we can expect Congress to investigate and "fact-find" in a thorough manner to better inform the process. And going back to the previous question – because nearly every Committee in Congress can lay claim to privacy being within its jurisdiction, it would not surprise me if nearly every Committee's oversight priorities have some sort of privacy nexus. ▪

For additional information, please contact:

Peter S. Hyun
202.719.4499 | phyun@wileyrein.com

The First Amendment Right to Political Privacy, Chapter 8 — A Postscript on The Individual and Social Costs of Compelled Disclosure

By Lee E. Goodman

This series has attempted to illuminate the legal principles at stake through the real experiences of the people who, at great personal expense, forged the First Amendment right of political conscience. That they suffered profound invasions of personal liberty guaranteed to them by the Bill of Rights is established by the court decisions. But they suffered severe personal pain too. Some were arrested and went to prison. Even those who ultimately prevailed in the legal system did so at great personal, financial, and psychological cost.

These kinds of individual experiences impose a collective injury to the democracy at large. John Stuart Mill in his treatise *On Liberty*, published in 1859, articulated the concept of a collective social cost to society that results from the loss of individual freedom in thought and speech.[1] When the cost of participating in the exchange of ideas becomes so high that individuals choose not to participate, to censor themselves, everyone is poorer collectively. They are poorer because they are denied the freedom to hear or even to think the ideas that might otherwise have enriched democratic debate, society, and themselves personally.

Thus, when compelled exposure causes individuals to refrain from speaking or joining associations, or funding a cause, because exposure carries too high a price in the form of stigma, boycotts, ignominy, harassment, law enforcement, or other official or social retaliation, the deterrence of individuals becomes a collective problem. There is a cost to democracy and society at large when individuals speak or associate less and share fewer ideas.

Regrettably, the censorship of ideas and the banishment of certain speakers often has been the specific purpose of public exposure campaigns and the transparency policies that facilitate those campaigns. And, indeed, such initiatives have been ecumenical throughout history, being employed by all parts of the political spectrum. New Deal Democrats harassed Edward Rumely's Committee on Constitutional Government for the better part of a decade in the 1940s. Southern government officials exposed NAACP donors through various registration requirements in order to deter their political participation. In the 1980s, a persistent Assistant School Superintendent doggedly pursued Margaret McIntyre to embarrass her in the local community, penalize her, and punish her for opposing the school funding referendum he favored.

In his book *Naming Names*, the definitive liberal treatise on the Red Scare, author Victor Navasky documents the painful personal toll suffered by hundreds of Hollywood artists when "informers" complied with formal government demands to "name names" in the 1940s and 1950s.[2] The personal consequences ranged from boycotts, unemployment, and economic ruin to deep personal traumas and suicide.[3] But "the state did more than bring misery to the lives of hundreds of Communists, former Communists, fellow travelers, and unlucky liberals," Navasky observes.[4] "It weakened American culture."[5] Navasky records the collective experiences and consequences of hundreds of American citizens as the "social cost" to government-compelled naming of names.[6]

The excesses of the Red Scare in the 1940s and 1950s were defended by conservatives of the day as an ordinary incident of democracy setting cultural and political norms.[7] But Judge Edgerton, the dissenter in the *Barsky* decision, saw the enterprise as something more insidious. He saw compulsory "exposure and publicity" as a weapon of ideological warfare against ideological opponents to accomplish what could not be done by direct legislation – censorship.[8]

continued on page 10

The First Amendment Right to Political Privacy, Chapter 8 — A Postscript on The Individual and Social Costs of Compelled Disclosure

Continued from page 9

The New Left of the 1960s responded with its own counter-speech theories and tactics that have been taken up by a new generation of Americans determined to censor right-leaning speakers and even left-wing speakers perceived as out-of-step with new progressive orthodoxy.[9]

The modern censorship movement extends to college campuses where "de-platforming" non-conforming viewpoints is commonplace,[10] to boycotts against advertisers on certain media outlets and news shows,[11] to affirmative efforts to block former government officials from employment at any corporation in America.[12] At the same time, official governmental discrimination against certain viewpoints and speakers appears to be as active as ever.[13] Two recent books, Kim Strassel's *The Intimidation Game* and Kirsten Powers' *The Silencing*, document the new political strategy in action.[14] And compulsory exposure is identified, like it was in the 1940s and 1950s, as a key tool of the conscious political strategy to drive ideological competitors out of the public square.[15]

Meanwhile, several books and studies document the rising intolerance in civic discourse and social cost in terms of the censorship of ideas and facts from public dialogue.[16] The intensity of protests and the severity of the intolerance that characterizes debate over even mundane political subjects today have pushed many citizens out of the public dialogue. Others have sought to participate anonymously not for the purpose of corrupting politicians but to protect their families, reputations, and careers. That in turn has spawned the most expansive and intrusive compulsory exposure laws and legislation, often justified, like historical precursors, in the name of transparency and national security.[17]

All forms of compelled exposure necessarily chill free speech and association. Public exposure chills some, while the risk of government abuse chills others. Although the risk can be more acute if the subject is controversial, or the viewpoint is unorthodox, or if the times, like the 1940s *and today*, are deeply polarized culturally and politically, all forms of government-compelled disclosure visit a chill upon citizens who otherwise would prefer to maintain their privacy while speaking or associating. As observed by Judge Edgerton at the height of the Red Scare, "There has been some suggestion that it restrains only timid people. I think it nearer the truth to say that, among the more articulate, it affects in one degree or another all but the very courageous, the very orthodox, and the very secure. But nothing turns on this question of fact. The views of timid people are not necessarily worthless to society. No one needs self-expression more. The Constitution protects them as it protects others."[18]

The courts have the responsibility to referee the modern ideological and cultural wars waged with the cudgel of government-compelled exposure and to draw boundaries upon compelled disclosure. The real consequences for individuals' lives and liberties, as well as the collective social costs to society, of compelled exposure must figure into a jurisprudence that seems to have forgotten or underrated these costs. Perhaps the courts in these turbulent and intolerant times will fulfill the hope of Justice Black, who at the height of the Red Scare longed for "calmer times, when present pressures, passions and fears subside" to afford the privacy of political conscience appropriate constitutional protection. ▪

For more information on the First Amendment right of political privacy, please contact:

Lee E. Goodman
202.719.7378 | lgoodman@wileyrein.com

continued on page 11

The First Amendment Right to Political Privacy, Chapter 8 — A Postscript on The Individual and Social Costs of Compelled Disclosure

Continued from page 10

Endnotes

[1]John Stuart Mill, *On Liberty* (Dover Publications 2002).

[2]Victor S. Navasky, *Naming Names* (Viking Press 1980).

[3]*Id.* at pp. 340-350.

[4]*Id.* at 334.

[5]*Id.*

[6]*Id.*

[7]*See* William F. Buckley, Jr., L. Brent Bozell, "The New Conformity," *McCarthy And His Enemies* (Henry Regnery Co. 1954) at pp. 308-330.

[8]*Barsky v. United States*, 167 F.2d 241, 256 (D.C. Cir. 1948) (Edgerton, *dissenting*).

[9]For the New Left's ideological origin, *see* Herbert Marcuse, "Repressive Tolerance," *A Critique of Pure Tolerance* (Beacon Press 1969) at pp. 95-137. The chapter was first published in 1965 and it forms the foundation for today's strategy of affirmative intolerance to free speech by the New Left. For a response to the theory and a documentation of the social cost in the form of heightened levels of intolerance in a generation of Americans, *see* April Kelly-Woessner, *The End of the Experiment* (ed. Stanley Rothman) (Routledge 2017) at pp. 187-200. For examples of New Left attacks on out-of-step liberal speakers, *see* Edward Schlosser, "I'm a Liberal Professor, and My Liberal Students Terrify Me," *Vox.com* (June 3, 2015); Jeremy Bauer-Wolf, "ACLU Speaker Shouted Down at William & Mary," *Inside Higher Ed* (Oct. 5, 2017).

[10]Paul Bedard, "Efforts to Blacklist Conservatives at UVA Persists, Trump Aide Hiring Defended," *The Washington Examiner* (Aug. 3, 2018); Greg Lukianoff, *Unlearning Liberty: Campus Censorship and the End of American Debate* (Encounter Books 2012); Foundation for Individual Rights in Education (FIRE) "Disinvitation Database" (available at: **https://www.thefire.org/resources/disinvitation-database/**).

[11]Itay Hod, "Tucker Carlson and Laura Ingraham Boycotts Have Cost Their Fox News Shows Millions, Data Shows," *TheWrap.com* (Feb. 5, 2019).

[12]*See* Gideon Resnick, "We're Not Finished, Dem Groups Want to Make Kirstjen Nielsen a Post-Trump Pariah," *TheDailyBeast.com* (Apr. 8, 2019) ("Restore Public Trust and nearly 40 immigration and progressive advocacy groups had formed a coalition to implore corporate leaders to avoid hiring a slew of Trump officials involved in implementing the family separation policy including Nielsen, former Attorney General Jeff Sessions and former White House Chief of Staff John Kelly.").

[13]*See, e.g.,* Emily Cochrane, "Department of Justice Settles With Tea Party Groups After I.R.S. Scrutiny," *The New York Times* (Oct. 26, 2017); Bradley Smith, "A Lesson on Abuse of Power by Obama and His Senate Allies," *The Hill* (Oct. 10, 2017); Karl Rove, "Dick Durbin, The IRS, and Me," *Wall Street Journal* (Mar. 29, 2013); Editorial, "Smart-ALEC Durbin Targets Another Conservative Group," *Investor's Business Daily* (Aug. 12, 2013); Laura Vozella, "McAuliffe Camp Erupts Over Business PAC's Choice of Cuccinelli for Virginia Governor," *Washington Post* (Sept. 15, 2013) (reporting on state senator's email to business association: "I urge you to stop any endorsement of Cuccinelli. The ramifications of his being endorsed will be huge within the Senate Democratic caucus…. The response [from legislators] will be frigid and doors will be closed [when the council seeks help with its legislative agenda]. Achieving the goals of NVTC will be difficult to impossible."); John Cushman, Jr., "Think Tank With Fossil-Fuel Ties Subpoenaed in AG's Climate Inquiry," *Inside Climate News* (Apr. 8, 2106).

[14]Kimberley Strassel, *The Intimidation Game; How the Left is Silencing Free Speech* (Twelve, The Hachette Book Group 2016); Kirsten Powers, *The Silencing: How the Left is Killing Free Speech* (Regnery Publishing 2015).

[15]Strassel, *The Intimidation Game* at pp. 64-65; *see also* 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) at pp. 8-9.

[16]April Kelly-Woessner, *The End of the Experiment* (ed. Stanley Rothman) (Routledge 2017) at pp. 187-200; Greg Lukianoff, *The Coddling of the American Mind* (Penguin Press 2018).

[17]*See, e.g.*, Honest Ads Act (S. 1989, 115th Congress); Maryland Online Electioneering Transparency and Accountability Act (Md. Code Ann., Elec. Law § 13-405.2); New York Democracy Protection Act (N.Y. Elec. Law § 14-107(5-a)); 13 N.Y.C.R.R. 91.5(C)(3)(1)(a); California Supervision of Trustees and Charitable Trusts Act (Cal. Govt. Code § 12584).

[18]*Barsky*, 167 F.2d at 255 (Edgerton, *dissenting*).

Chambers USA Recognizes Wiley Rein Privacy, Cyber & Data Governance Practice Attorneys as Among Best in the Country

The 2019 edition of *Chambers USA*: *America's Leading Lawyers for Business* has recognized Wiley Rein's Privacy, Cyber & Data Governance practice as a nationwide leader. Chambers also acknowledges partner Megan Brown as a Recognized Practitioner in the field.

Chambers acknowledges the practice for its "impressive work in healthcare privacy matters" and notes that it is considered highly adept at handling data breaches. Chambers also highlights the Firm's expertise in tax privacy, international and EU data transfer matters, and electronic surveillance and law enforcement, and notes that Firm attorneys are frequently called on for advice on regulatory compliance issues, including HIPAA.

Chambers notes that sources say: *"They provide very practical legal advice on topics that are usually time-sensitive. They have a strong bench and are very practically oriented, but also have a good view of government data and security. They also understand the litigation aspects that could develop and are strong on governance.*"

Additionally: *"Their subject matter expertise is superior and if they do not have a specific expertise, they get it."* And clients value that *"they are very responsive and offer a real depth of experience."*

The 2019 edition of *Chambers USA*: *America's Leading Lawyers for Business* recognizes 31 Wiley Rein attorneys across 12 areas of law. The practices ranked as leaders nationwide are **Election Law & Government Ethics**, **Government Contracts**, **International Trade**, and **Privacy, Cyber & Data Governance**. The practices ranked as leaders in Washington, DC, are **Insurance**, **Media**, and **Telecom, Media & Technology**.

In addition, Wiley Rein is listed as a "Recognized Practitioner" for **Environment**, **Litigation: White Collar Crime & Government Investigations**, **Franchising**, and International Trade: **Export Controls** & **Economic Sanctions**.

Events & Speeches

IoT Security: Aligning International Responses to Shared Risks
U.S. Chamber of Commerce
Megan L. Brown
May 3, 2019 | Washington, DC

Policing the Blockchain: Protecting Investors and Consumers
Consensus 2019
Duane C. Pozza, Speaker
May 15, 2019 | New York, NY

NAAG Consumer Protection Spring Conference
Kevin G. Rupy, Speaker
May 20, 2019 | Washington, DC

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

Robocalling Enforcement: Procedures and Penalties
Federal Communications Bar Association
Kevin G. Rupy, Speaker
June 10, 2019 | Minneapolis, MN

2019: The Pivotal Year in the Battle Against Illegal Robocalls
Communications Fraud Control Association
Kevin G. Rupy, Speaker
June 13, 2019 | Minneapolis, MN

2019: The Pivotal Year in the Battle Against Illegal Robocalls
4th Annual U.S.-India Business Council and Federal Trade Commission Workshop
Kevin G. Rupy
June 20, 2019 | Washington, DC

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

Privacy and Cybersecurity at Wiley Rein

Rachel A. Alexander	202.719.7371	ralexander@wileyrein.com
Megan L. Brown	202.719. 7579	mbrown@wileyrein.com
Moshe B. Broder	202.719.4186	mbroder@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
Michael L. Diakiwski	202.719.4081	mdiakiwski@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
Kevin G. Rupy	202.719.4510	krupy@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.*