Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | September 2019

While we wait for Congress to act on privacy and cybersecurity legislation – and comb through the latest state developments – federal agencies are moving forward in critical ways that are often less publicized but still affect industry. We start this issue discussing the U.S. Department of Homeland Security's latest strategic document on cybersecurity in critical infrastructure operated by private companies, including cutting-edge 5G technology, in an article by Megan Brown and Michael Diakiwski.

Next up, Jackie Ruff and I discuss the federal government's latest work on artificial intelligence (AI) standard-setting, which will become increasingly important as the Executive Branch maps out its regulatory approach to AI across numerous sectors. Kat Scott and Megan Brown analyze NIST's draft of its Privacy Framework – a key development in the federal approach to privacy. And we discuss the FTC's announcement of a coming sweep of internet content directed to children for potential privacy violations, in an article by myself, Antonio Reynolds, Joan Stewart, Megan Brown, and Scott Delacourt. The "In Brief" section provides additional updates on some of our commentary in the areas of political disclosures, privacy regulations, and robocalls.

Feel free to reach out to me or any of the other authors with feedback or questions. I can be reached at 202.719.4533 or dpozza@wileyrein.com. Thank you as always for reading.

-Duane Pozza, Partner, Privacy, Cyber & Data Governance Practice

IN THIS ISSUE:

Homeland Security Focuses on Private Sector Engagement on Emerging Threats to Critical Infrastructure

By Megan L. Brown and Michael L. Diakiwski

As next-generation wireless technologies are deployed and adopted, technology and telecommunications companies should be prepared for long-term engagement with the federal government on security issues, especially with the U.S. Department of Homeland Security (DHS). The Department has long recognized that the private sector controls and manages most of the country's critical infrastructure,[1] and it emphasizes the significant importance of public-private partnerships and coordinated risk management across government and the private sector. Within DHS, the Cybersecurity and Infrastructure Security Agency (CISA) leads the federal effort to help safeguard the nation's critical

continued on page 2

Homeland Security Focuses on Private Sector Engagement on Emerging Threats to Critical Infrastructure

Continued from 1

infrastructure from both cyber and physical threats and vulnerabilities. These efforts are largely voluntary, in collaboration with other government and private-sector stakeholders.2

At the end of August 2019, CISA released its *Strategic Intent*, which calls for sustained public-private collaboration. According to CISA, "this document lays out the strategic vision and operational priorities of the CISA Director."3 It outlines the agency's mission to "lead the national effort to understand and manage cyber and physical risk to our critical infrastructure" and overall vision for a more "secure and resilient critical infrastructure for the American people."4

The *Strategic Intent*'s first guiding principle outlines that: "Without successful collaboration with our partners, we cannot achieve our mission. Our approach will drive conversation about the problem and potential solutions and will require new models of partnership."5

Notably, among the CISA Director's key operational directives, the first stated priority is "China, Supply Chain, and 5G":

> China presents the most pressing long-term strategic risk to the United States. The persistent threat posed by China compels CISA's focus on supply chain risk management in the context of national security. CISA is looking to reduce the risks of Chinese supply chain compromise, whether that is through 5G or any other technologies.6

The document formalizes and builds upon numerous lines of effort that CISA has launched to secure cyber and communications infrastructures, many of which require and rely upon dynamic participation from the private sector.

Addressing Systemic Risks

CISA's National Risk Management Center (NRMC) is a planning, analysis, and collaboration center working to identify and address the most significant risks to the nation's critical infrastructure. The NRMC works in close coordination with the private sector and other key stakeholders in the critical infrastructure community.7 In early 2019, the NRMC produced a list of "national critical functions,"8 which are divided into four different areas: (1) *Supply*, which focuses on providing resources to the public; (2) *Distribute*, which has a heavy focus on the movement of goods and people; (3) *Manage*, which is the largest bucket with a variety of functions; and (4) *Connect*, which focuses on communications and internet services.9

CISA maintains close ties with certain critical infrastructure sectors, including the Communications and Information Technology Sectors. CISA established the Tri-Sector Executive Working Group, consisting of senior leaders from the financial services, communications, and electricity communities, working together to manage known and emerging risks. Activities are underway to help direct intelligence collection requirements, build cross-sector risk management playbooks, and better understand and address systemic risk.10

Supply Chain, 5G, and Emerging Technologies

CISA "is committed to working with government and industry partners to ensure that supply chain risk management is an integrated component of its cybersecurity efforts."11 The agency's Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force is a public-private partnership with more than 20 federal partners and over 40 private-sector company representatives focused on four main work streams, including:

- Developing a common framework for the bi-directional sharing of supply chain risk information between government and industry;
- Identification of processes and criteria for threat-

continued on page 3

Homeland Security Focuses on Private Sector Engagement on Emerging Threats to Critical Infrastructure

Continued from 2

based evaluation of ICT supplies, products, and services;

- Identification of market segment(s) and evaluation criteria for Qualified Bidder and Manufacturer List(s); and,

Producing policy recommendations to incentivize the purchase of ICT from original manufacturers or authorized resellers.12

CISA, as noted in its *Strategic Intent*, is preparing to respond to the threats of tomorrow including those in the next generation of wireless technology or "5G." The agency notes that:

[5G] connections will empower a vast array of new and enhanced critical services, from autonomous vehicles and telemedicine, to automated manufacturing and advances to traditional critical infrastructure, such as smart grid electricity distribution. Given 5G's scope, the stakes for safeguarding these vital networks could not be higher. CISA is leading risk mitigation efforts across the federal government and is committed to working with government and industry partners to ensure the security and integrity of 5G technology in our nation.13

As part of these mitigation efforts, CISA collaborated with industry representatives to develop an *Overview of Risks Introduced by 5G Adoption in the United States* and related *5G Infographic*.14 This document states that the U.S. government can manage vulnerabilities by "encouraging the continued development of trusted 5G technologies, services, and products" and "continued engagement with the private sector on risk identification and mitigation efforts," among other things.15

In May, the President issued the *Executive Order on Securing the Information and Communications Technology and Services Supply Chain*. DHS, through CISA and other collaborating offices, was required to "assess and identify entities, hardware, software, and services that present vulnerabilities in the United States and that pose the greatest potential consequences to the national security of the United States."16 This assessment was developed "in coordination with sector-specific agencies and coordinating councils as appropriate."17 The risk assessment is being used to inform the U.S. Department of Commerce as it develops rules called for by the *Executive Order*.

Looking Ahead

On September 18 – 20, CISA hosted the second annual National Cybersecurity Summit, to "bring together critical infrastructure stakeholders from around the world to a forum with presentations focused on emerging technologies, vulnerability management, incident response, risk mitigation, and other current cybersecurity."18 Like the first Summit held in 2018, this event underscores the Department's view that cybersecurity, and national security more broadly, is a shared responsibility – one in which critical infrastructure operators, including technology and communications companies, play a central role. As DHS states, the Summit provided the opportunity for [government] agencies, private sector organizations, and international partners to highlight successes and opportunities for collective action.19

For CISA, now and into the future, collaborative and iterative risk assessments will need to leverage private-sector knowledge and expertise. The private-sector companies providing innovative technologies and communications products and services should expect and be prepared to engage with the Department, as it wrestles with ever-evolving security challenges. ▪

For additional information, please contact:

Megan L. Brown
202.719.7579 | mbrown@wileyrein.com

Michael L. Diakiwski
202.719.4081 | mdiakiwski@wileyrein.com

continued on page 4

Homeland Security Focuses on Private Sector Engagement on Emerging Threats to Critical Infrastructure

Continued from 3

ENDNOTES

[1] See DHS, Critical Infrastructure Sectors ("There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."), available at: https://www.dhs.gov/cisa/critical-infrastructure-sectors.

[2] DHS, CISA, Supporting Policy and Doctrine, available at: https://www.dhs.gov/cisa/supporting-policy-and-doctrine.

[3] DHS, CISA Strategic Intent – Defend Today, Secure Tomorrow (August 2019), available at: https://www.dhs.gov/publication/cisa-strategic-intent. ("CISA Strategic Intent").

[4] CISA Strategic Intent at 5.

[5] Id.

[6] CISA Strategic Intent at 8.

[7] See DHS, CISA, National Risk Management Center, available at: https://www.dhs.gov/cisa/national-risk-management.

[8] See DHS, National Critical Functions: An Evolved Lens For Critical Infrastructure Security and Resilience, available at: https://www.dhs.gov/sites/default/files/publications/national-critical-functions-overview-508.pdf (National Critical Functions are defined as: "The functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.").

[9] See DHS, CISA, National Critical Functions Set, available at: https://www.dhs.gov/cisa/national-critical-functions-set.

[10] See CISA Strategic Intent at 12; see also DHS, CISA, Tri-Sector Executive Working Group, available at: https://www.dhs.gov/cisa/tri-sector-executive-working-group.

[11] DHS, CISA, Supply Chain Risk Management available at: https://www.dhs.gov/cisa/supply-chain-risk-management.

[12] DHS, CISA, Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force, available at: https://www.dhs.gov/cisa/information-and-communications-technology-ict-supply-chain-risk-management-scrm-task-force.

[13] DHS, CISA, 5G Adoption in the United States, available at: https://www.dhs.gov/cisa/5g.

[14] DHS, CISA, Overview of Risks Introduced by 5G Adoption in the United States, available at: https://www.dhs.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf.; see also DHS, CISA, 5G Infographic: 5G Wireless Networks Market Penetration and Risk Factors (July 2019), available at: https://www.dhs.gov/sites/default/files/publications/pdm19028_5g_risk_characterizationc_v14_05july2019.pdf.

[15] See id at 1.

[16] President Donald J. Trump, Executive Order on Securing the Information and Communications Technology and Services Supply Chain (May 15, 2019), available at: https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

[17] Id.

[18] DHS, CISA, a 2019 CISA Cybersecurity Summit, available at: https://www.us-cert.gov/event/2019-cisa-cybersecurity-summit.

[19] Id.

NIST's Plan for Federal AI Standards Points to Industry Involvement

On August 12, the National Institute of Standards and Technology (NIST) announced the release of its long-anticipated Plan for federal engagement and U.S. leadership on artificial intelligence (AI) standards. The Plan sets out a framework for federal agencies to move forward on developing AI standards that will be critical to both U.S. and international regulatory and policy approaches. And it makes industry engagement a centerpiece of federal efforts, particularly as the U.S. government attempts to work globally to shape AI standards with countries that share a similar pro-innovation approach.

The Plan has four main recommendations:

- Bolster AI standards for leadership and coordination among agencies;
- Promote focused research to help support "trustworthy" AI;
- Support and expand public-private partnerships on AI; and
- Strategically engage with international parties to advance AI standards for U.S. economic and national security needs.

Standards Development

The Plan identifies nine categories of AI standards for further development. These include a number of standards that will be important as regulatory approaches evolve.

Some of the more substantive regulatory standards respond to issues that have repeatedly come up in regulatory and policy debates around AI. For example, standards will address data quality, privacy, safety, security, risk management, explainability, and "objectivity," which appears to cover issues around bias. These can form the foundation of regulatory approaches by defining an optimal outcome for regulation. For example, what does it mean for AI outcomes to be "explainable" when AI algorithms can learn as they go? As the Plan recognizes, work is already being done in some of these areas but more industry input is needed.

Agencies Leading the Standards Work

The Plan largely directs individual agencies to drive standards-setting in individual sectors. NIST recommends that each agency should assess how AI can be used to further the agency's mission, conduct a "landscape scan and gap analysis" to identify standards that need to be developed, and engage in standards development if necessary. The plan points to the U.S. Department of Transportation (DOT) and the U.S. Food and Drug Administration (FDA) as being "ahead of the curve." DOT for example has issued guidance (AV 3.0) on its approach to autonomous vehicles and safety.

Additionally, the Plan establishes a few centralized areas of coordination on the domestic front:

National Science and Technology Council (NSTC): NIST recommends that the NSTC Machine Learning/AI Subcommittee establish a Standards Coordinator who will gather and share standards strategies and best practices across agencies. The Coordinator will identify specific areas for prioritization, ensure coordination with private sector standards development organizations (SDOs), and determine whether additional guidance is appropriate.

Office of Management and Budget (OMB): NIST recommends that OMB "[r]einforce the importance of agencies' adherence to Federal policies for standards and related tools," including in the area of data access.

NIST / U.S. Department of Commerce: NIST will take the lead on developing metrics, data sets, and benchmarks to assess reliable and "trustworthy" attributes of AI systems, and identify research needs for related scientific breakthroughs. And along with the National Science Foundation, it will facilitate research and collaboration on societal and

continued on page 6

NIST's Plan for Federal AI Standards Points to Industry Involvement

Continued from 5

ethical considerations that might bear on the use of standards.

Importance of Industry Engagement and Public/Private Partnerships

Overall, the Plan envisions that agencies will work collaboratively with industry in engaging in standards-setting processes. This approach relies "largely on the private sector to develop voluntary consensus standards, with Federal agencies contributing to and using those standards."

The Plan directs agencies to prioritize standards-setting efforts that are "consensus-based," open and transparent, and globally non-discriminatory. And the plan encourages those efforts to be (among other things) innovation-oriented, regularly updated, human-centered, and applicable across sectors, but also focused on specific sectors where there are specific risks.

International Engagement

Finally, the Plan recommends that the U.S. government escalate its efforts, likely in partnership with industry, to shape AI technical standards and other policies globally. The Plan identifies the U.S. Departments of Commerce, State, and Justice as the lead agencies on international engagement. This priority – coupled with increased interest in Europe and elsewhere in AI regulation – points to the need for businesses to develop policy positions and advocate with these agencies.

In particular, the Plan includes a recommendation to "champion U.S. AI standards priorities" around the world. This will likely result in increased involvement by the U.S. government in global AI standards development, such as international SDOs like the International Organization for Standardization (ISO) and U.S.-based organizations like the IEEE that create standards for global use. The Plan notes that some governments play a more centrally managed role in standards development and related activities, and it emphasizes that the government should "ensure that U.S. standards-related priorities and interests . . . are not impeded." Thus, it will be important for industry to ensure U.S. agencies are aware and supportive of business priorities, and industry should be prepared for government requests for technical expert input and increased participation in standards-setting activities.

The Plan also recommends that the U.S. develop AI standards collaboratively with "like-minded countries." U.S. support for the Organisation for Economic Co-operation and Development's (OECD) AI principles is a good example of this approach, and many policy debates outside the U.S. are now moving into a more detailed phase of implementation of high-level principles from the OECD and from the European Commission (EC). Notably, the OECD and EC frameworks apply compliance expectations throughout the AI ecosystem, including to both AI developers and users.

▪ ▪ ▪

Overall, NIST has created a framework that opens the door for industry leadership in driving the formation of key AI standards like explainability, bias, accuracy, risk management, and safety. Well-developed and thoughtful standards in those areas can promote innovation in an exciting and quickly moving area. Our AI team at Wiley Rein continues to engage with key government stakeholders as the process moves forward. ■

For additional information, please contact:

Duane C. Pozza
202.719.4533 | dpozza@wileyrein.com

Jacquelynn Ruff
202.719.7224 | jruff@wileyrein.com

Breaking Down NIST's Draft Privacy Framework

By Kathleen Scott and Megan L. Brown

Slightly shy of a year from kicking off the Privacy Framework effort, the National Institute of Standards and Technology (NIST) has released a preliminary draft of the document, entitled *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management* (Draft Framework or Draft). This Draft comes amidst a continued flurry of privacy activity at both the state and federal levels.

The Draft Framework is intended to help organizations understand, communicate, and manage privacy risks. The document is "agnostic to any particular technology, sector, law, or jurisdiction"[1] and is meant to be a practical implementation tool for organizations to manage risks. In short, while other parts of the federal government are considering various privacy policy approaches, NIST's goal has been "to deliver a tool that could help organizations communicate better about privacy risks when designing and deploying products and services, provide more effective solutions that can lead to better privacy outcomes, and facilitate compliance with their legal obligations."[2]

Below is what you need to know about the Draft Framework, as well as next steps for engagement.

The Framework Basics: Like NIST's popular Cybersecurity Framework, the Draft Framework has 3 main parts: the Core, Profiles, and Implementation Tiers.

- **The Core** consists of 5 high-level "privacy protection activities and outcomes" known as Functions:[3] Identify-P, Govern-P, Control-P, Communicate-P, and Protect-P. The first 4 Functions are intended to help to manage privacy risks that arise from data processing, and the final Function is intended to help manage privacy risks that arise from privacy breaches. However, NIST makes clear that the final Function, Protect-P, is "not the only way to manages privacy risks associated with privacy breaches," and that organizations can use the Privacy Framework in conjunction with the Cybersecurity Framework to address privacy and cybersecurity risks together.[4] Additionally, each Function has corresponding Categories and Subcategories of various privacy outcomes.

Table 1: Privacy Framework Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID-P	Identify-P	ID.IM-P	Inventory and Mapping
		ID.BE-P	Business Environment
		ID.RA-P	Risk Assessment
		ID.DE-P	Data Processing Ecosystem Risk Management
GV-P	Govern-P	GV.PP-P	Governance Policies, Processes, and Procedures
		GV.RM-P	Risk Management Strategy
		GV.AT-P	Awareness and Training
		GV.MT-P	Monitoring and Review
CT-P	Control-P	CT.PO-P	Data Management Policies, Processes, and Procedures
		CT.DM-P	Data Management
		CT.DP-P	Disassociated Processing
CM-P	Communicate-P	CM.PP-P	Communication Policies, Processes, and Procedures
		CM.AW-P	Data Processing Awareness
PR-P	Protect-P	PR.AC-P	Identity Management, Authentication, and Access Control
		PR.DS-P	Data Security
		PR.DP-P	Data Protection Policies, Processes, and Procedures
		PR.MA-P	Maintenance
		PR.PT-P	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

- **A Profile** is an organization's selection of specific Functions, Categories, and Subcategories, based on the organization's "business requirements, risk tolerance, privacy values, and resources," and other factors, such as "legal/regulatory requirements and industry best practices."[5] NIST makes clear that an organization "may not need to achieve every outcome or activity reflected in the Core"

continued on page 8

Breaking Down NIST's Draft Privacy Framework

Continued from 7

and that instead, and organization may tailor the Framework when developing its Profile or Profiles.6

- Implementation Tiers "support organizational decision-making about how to manage privacy risk by taking into account the nature of the privacy risks engendered by the organization's systems, products, or services and the sufficiency of the processes and resources the organization has in place to manage such risks."7 NIST reiterates that the Tiers should not be thought of as maturity level; in fact, as NIST describes, Tier 2 could be sufficient for some organizations.

Key Characteristics of the Framework: The Draft Framework proposes a **voluntary** and **flexible** tool for organizations to manage privacy risk. These characteristics support NIST's goal for the document to be "widely usable by organizations of all sizes."8 In its drafting, NIST makes clear that "managing risks to individuals' privacy is not well-suited to a one-size- fits-all solutions,"9 so it explains that "[t]he Privacy Framework . . . is flexible enough to address diverse privacy needs, enable more innovative and effective solutions that can lead to better outcomes for individuals and enterprises, and stay current with technology trends, including [AI and IoT]."10

How to Use the Framework: Further driving the characteristic of flexibility, NIST highlights that "[d]ifferent types of entities . . . can use the Privacy Framework for different purposes."11 Depending on the "unique needs of an organization,"12 some potential uses include: mapping to Informative References, strengthening accountability within the organization, establishing or improving privacy programs, and informing buying decisions, among others.

Next Steps: The current Draft Framework is open for public comment, with comments due by October 24. NIST has welcomed feedback on the Framework from the start of this process, but the opportunity for interested stakeholders to weigh in is winding down, as NIST hopes to finalize the Privacy Framework by the end of the year. If your organization would like to engage with NIST on this important document, now is the time! ■

For additional information, please contact:

Megan L. Brown
202.719.7579 | mbrown@wileyrein.com

Kathleen E. Scott
202.719.7577 | kscott@wileyrein.com

[1] Draft Framework at 4.

[2]Naomi Lefkovitz, *The Preliminary Draft of the NIST Privacy Framework is Here!*, Cybersecurity Insights—a NIST blog (Sept. 9, 2019), https://www.nist.gov/blogs/cybersecurity-insights/preliminary-draft-nist-privacy-framework- here.

[3] Draft Framework at 5.

[4] *Id.*

[5] *Id.* at 10-11.

[6] *Id.*

[7] *Id.* at 12.

[8] *Id.* at 4.

[9] *Id.* at 3.

[10] *Id.* at 3.

[11] *Id.*at 9

[12] *Id.* at 12.

FTC Announces Upcoming COPPA Sweep of Online Content Uploaders Following YouTube Settlement

By Duane C. Pozza Antonio J. Reynolds, Joan Stewart, Megan L. Brown, and Scott D. Delacourt

On September 4, 2019, the FTC took major action under the Children's Online Privacy Protection Rule (COPPA), adopting an aggressive posture toward online platforms and content creators. The FTC announced a major COPPA settlement with YouTube, coupled with a promised sweep of online content uploaders – which its order calls "channel owners" – for COPPA compliance. These actions, and the FTC's accompanying statements, signal a paradigm shift in enforcement for private companies that create, distribute and host material online.

The FTC settlement, which included the New York Attorney General, requires YouTube to implement a system for content uploaders to designate whether content is child-directed under COPPA. The FTC stated that it will review the accuracy of those designations, as part of a broader policing of online platforms and content providers for COPPA compliance.

By way of background, COPPA requires that operators of websites or online services directed to children younger than 13, and other websites or online services that have actual knowledge that they are collecting personal information from a child younger than 13, to comply with certain obligations including parental notice and consent.

When a user uploads content to an online platform like YouTube, the platform often assigns a persistent identifier to users who view the content and collects information about what other content the user views for purposes of targeted advertising. This raises potential COPPA concerns because persistent identifiers are considered personal information covered under the COPPA Rule's parental notification and consent requirements.

Section I of the settlement order with YouTube requires the company to develop, implement, and maintain a system for channel owners to designate whether their content on the YouTube service is directed to children. The company must also provide a clear and conspicuous notice to channel owners that that their content may be subject to COPPA and that channel owners are obligated to designate such content as directed to children. A "channel owner" is broadly defined as anyone who uploads videos onto the service.

In his remarks, FTC Chairman Joseph Simons emphasized that the settlement was meant to send a message to content uploaders to ensure their compliance with COPPA, and noted that a sweep of content owners would be conducted after the settlement had been "effective for a period of time." An advance announcement of a sweep is unusual for the FTC, and must be taken seriously. If the FTC believes that some content is not being designated as child-directed and there is a potential COPPA violation, it can send extensive Civil Investigative Demands to companies, and potentially bring enforcement actions with fines in the many millions of dollars. State attorneys general also can investigate and bring suit, and have been increasingly active in COPPA enforcement.

In light of the FTC's announcement, we expect further action on COPPA enforcement. We are monitoring this area carefully and can be contacted for further assistance.

For additional information, please contact:

Duane C. Pozza
202.719.4533 | dpozza@wileyrein.com

Antonio J. Reynolds
202.719.4603 | areynolds@wileyrein.com

Joan Stewart
202.719.7438 | jstewart@wileyrein.com

Megan L. Brown
202.719.7579 | mbrown@wileyrein.com

Scott D. Delacourt
202.719.7459 | sdelacourt@wileyrein.com

In Brief

Lee Goodman Pens Op/Ed on Political Privacy

Lee E. Goodman, partner in Wiley Rein's Election Law & Government Ethics Practice, has penned a widely read editorial in The Hill titled "Honest Political Ads: Watch Out Drudge, You're Next."

https://thehill.com/opinion/cybersecurity/459896-honest-political-ads-watch-out-drudge-youre-next

Mr. Goodman addresses the adverse implications of the Honest Ads Act, a bill pending in Congress, for the political privacy and free speech rights of American citizens. He argues that American citizens would be chilled from discussing public policy issues under the bill's provision mandating that media and tech platforms collect and publish the names and addresses of advertisers who spend as little as $500 on ads discussing public policy. "When Congress returns to business next week, it will take up … the Honest Ads Act, a bill severely restricting the First Amendment rights of American citizens and media companies but barely impacting foreign meddlers," Goodman writes.

Mr. Goodman concludes that the Honest Ads Act would be ineffective at preventing foreign meddling in U.S. elections, which is its stated objective. He posits that Congress could more effectively confront foreign propaganda by amending the Foreign Agents Registration Act, a statute that regulates, but does not prohibit, the dissemination of foreign-sponsored information in the United States with appropriate disclaimers identifying the foreign sponsor.

Privacy in Focus previously covered the federal district court's decision in *The Washington Post v. McManus*, a ruling that enjoined Maryland's analog to the Honest Ads Act, because the law would force media companies to publish information about their advertisers that the media do not desire to publish [Federal Court Enjoins Maryland Internet Disclosure Law, But…]. Maryland has appealed that decision to the U.S. Court of Appeals for the Fourth Circuit [The Washington Post Resists Disclosure Burdens in the Fourth Circuit].

Lee Goodman can be reached at 202.719.7378 or lgoodman@wileyrein.com

---

Megan Brown Co-Authors National Security Institute's New Law and Policy Paper on 'Privacy Regulation and Unintended Consequences for Security'

Megan L. Brown, partner in Wiley Rein's National Security, Privacy, Cyber & Data Governance, and Telecom, Media & Technology practices, co-authored a new law and policy paper published August 14, 2019 by the National Security Institute (NSI) at George Mason University's Antonin Scalia Law School. The paper is co-authored with NSI Visiting Fellow James B. Burchfield.

The paper addresses:

- The federal urgency to act in response to public concern and the rapid global and domestic expansion of comprehensive privacy regulation.
- Implications privacy regulation can have for data protection and beneficial security activities.

continued on page 11

In Brief

Continued from 10

- The argument that artificial intelligence (AI), biometrics, and certain data categories are all critical to security innovations and activities and must be protected in privacy regulation.
- Actionable recommendations to ensure privacy regulation appropriately balances individual rights with security.

The paper is available here. The NSI press release can be found here.

Ms. Brown is an NSI Senior Fellow and Associate Director for Cybersecurity Programs.

Megan Brown can be reached at 202.719.7579 or mbrown@wileyrein.com.

Kevin Rupy Discusses Ways to Combat Illegal Robocalls on C-SPAN's "Washington Journal"

Kevin G. Rupy, partner in Wiley Rein's Telecom, Media & Technology(TMT) Practice, was interviewed by John McArdle of C-SPAN's "Washington Journal" for a program discussing industry and government efforts to address illegal robocalls, which aired Saturday, August 31.

Mr. Rupy, former Vice President of Law and Policy at the United States Telecom Association, began the discussion by noting the distinction between legal robocalls, such as those from pharmacies regarding prescriptions or notifications about school closings, versus illegal robocalls involving scams and fraudulent activity. He addressed a variety of topics regarding the complexity of the issue, and discussed the importance of bipartisan support, combined with involvement from the Federal Communications Commission and private industry.

"You're starting to see much greater collaboration between industry and government at both the federal and state level, and that collaboration is crucial to addressing this issue," said Mr. Rupy.

The video can be viewed here.

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

Speeches & Events

Robocall Regulatory Super-Session – Current Legislative and Regulatory Actions and Their Requirements and Ramifications.
The SIP Network Operators Conference "Focus on STIR/SHAKEN"
Kevin G. Rupy, Moderator
December 3, 2019 | Herndon, VA

Cybersecurity in the Internet of Things
U.S. Chamber of Commerce Global Cyber Dialogue
Megan L. Brown, Speaker
October 9, 2019 | Washington, DC

5G, Huawei, and National Security
Wiley Rein National Security Webinar + Podcast Series
Megan L. Brown, Speaker
September 12, 2019

Understanding Smart Contracts & How They Work
2019 SCG Legal Annual Meeting & 30th Anniversary Celebration
Duane C. Pozza, Speaker
September 6, 2019 | Washington, DC

When Congress Investigates: Breaking Down the Nuts and Bolts of Congressional Investigations
2019 FBA Annual Meeting & Convention
Peter S. Hyun, Panelist
September 5, 2019 | Tampa, FL

Webinar and Podcast Library

September 12, 2019
Wiley Rein Partners Megan Brown and Katy Ross, and NTIA's Acting Administrator, Diane Rinaldo, discuss 5G, Huawei, and National Security
Wiley Rein National Security Webinar + Podcast Series
Megan L. Brown, Katy M. Ross

July 18, 2019
The Latest Regulatory Developments in AI
Wiley Connected
Duane C. Pozza, Jacquelynn Ruff

July 17, 2019
Latest Update on State Privacy and Security Laws: California and Beyond
Wiley Rein Webinars
Duane C. Pozza, Matthew J. Gardner, Joan Stewart, Kathleen E. Scott

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

March 20, 2019
Mobile World Congress: A Discussion on 5G and the Future of the Mobile Industry
Wiley Connected
Scott D. Delacourt, Jacquelynn Ruff

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

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

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

January 7, 2019
Blockchain, Trust, and Regulation: A Conversation with Wharton Professor Kevin Werbach
Wiley Connected
Duane C. Pozza

November 30, 2018
Advanced Persistent Chats: DHS's Cybersecurity and Infrastructure Security Agency Podcast
Wiley Connected
Megan L. Brown, Michael L. Diakiwski

October 30, 2018
Podcast: How Much Do You Know About Blockchain Policy? An Interview with the Blockchain Association's Director of External Affairs, Kristin Smith
Wiley Connected
Matthew J. Gardner

Privacy and Cybersecurity at Wiley Rein

Rachel A. Alexander	202.719.7371	ralexander@wileyrein.com
Daniel P. Brooks	202.719.4183	dbrooks@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
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
Antonio J. Reynolds	202.719.4603	areynolds@wileyrein.com
Jacquelynn Ruff	202.719.7224	jruff@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.

To update your contact information or to cancel your subscription to this newsletter, visit:

www.wileyrein.com/newsroom-signup.html.