Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | December 2018

This month we introduce our new colleague, Duane Pozza, who joins us from the Federal Trade Commission (FTC). For his first *Privacy in Focus* contribution, Duane discusses the FTC's focus on potential types of "informational injuries" as the FTC reviews its approach to privacy and security enforcement. Lee Goodman continues his thought-provoking discussion of the First Amendment right to political privacy. Lastly, Michael Diakiwski, Megan Brown, and Kat Scott review the recent report from the U.S. Departments of Commerce and Homeland Security addressing a "Road Map" regarding botnets. As always, please let me know if you have questions or comments on any of these topics, or if we can be of assistance in connection with any of these developments. Please let me know if you have thoughts on topics you would like us to address in future issues of *Privacy in Focus*. I can be reached at 202.719.7335 or **knahra@wileyrein.com**. Thank you for reading. ■

— Kirk Nahra, Privacy & Cybersecurity Practice Chair

ALSO IN THIS ISSUE

FTC Focuses on Potential Types of 'Informational Injuries' as It Re-Examines Approach to Consumer Privacy

By Duane C. Pozza

As part of the Federal Trade Commission's (FTC) ongoing re-evaluation of its approach to consumer privacy, recent comments from FTC staff have emphasized the need to differentiate between different kinds of potential harms that might occur from disclosure of consumer information – and called for more empirical research on that question from stakeholders. A recent staff perspective paper on informational injuries and a comment to the National Telecommunications and Information Administration (NTIA) reiterate the Commission's approach to distinguishing different kinds of privacy-related harms as well as the call for

continued on page 9

Duane Pozza, Who Led FTC's Financial Technology Strategy, Joins Wiley Rein

Duane C. Pozza, former Assistant Director in the Division of Financial Practices at the Federal Trade Commission's (FTC) Bureau of Consumer Protection, has joined Wiley Rein's preeminent **Telecom, Media & Technology (TMT) Practice** as a partner. A leading lawyer with respect to technological innovation, consumer protection, and enforcement, Duane advises clients on key legal issues, advocacy positions, and regulatory compliance in such areas as blockchain, privacy and security, the Internet of Things (IoT), artificial intelligence (AI) and data analytics, mobile payments, and fintech lending. He authored the lead article in this issue of *Privacy in Focus*.

At the FTC, Duane was the go-to-attorney for financial technology matters and led strategy and enforcement on legal issues related to fintech. He led multiple agency initiatives on cutting-edge technologies including blockchain, AI, mobile payments, and other fintech innovations, focusing on issues including data security, privacy, fraud, and financial regulation. He also led and supervised numerous enforcement actions involving a range of consumer protection issues on technology platforms.

Duane Pozza can be reached at 202.719.4533 and **dpozza@wileyrein.com**.

Botnet 'Road Map' Tees Up Actions for Government and Industry

By Michael L. Diakiwski, Megan L. Brown, and Kathleen E. Scott

On November 29, 2018, the U.S. Departments of Commerce (DOC) and Homeland Security (DHS) released a **Road Map Toward Resilience Against Botnets** ("Road Map"). It builds upon and aims at implementing actions and recommendations from the report "*Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*" ("*Botnet Report*") published in May. The tasks identified in the Road Map tie together multiple streams of effort across government and industry. Many proposals are global in nature, will continue to evolve based on the threat environment, and – in order to be successful – require substantial participation from the private sector. In short, the Road Map envisions a long-term *whole-of-ecosystem* effort to mitigate the threat posed by botnets and distributed denial-of-service (DDoS) attacks.

Tasks range from identifying Internet of Things (IoT) security baselines, drafting procurement regulations, developing international IoT standards, and raising security awareness across the board. While the Road Map underscores that the

continued on page 3

private sector, as a whole, must shore up the security of its networks and systems, looking ahead, companies developing secure technologies and implementing best practices could have market growth opportunities – and the ability to help shape domestic and international security standards and expectations.

OVERVIEW AND BACKGROUND

The Road Map "charts a path forward, setting out steps to stop the cyber threat to our internet infrastructure. It outlines a plan for coordination among government, civil society, technologists, academics, and industry sectors to develop a comprehensive strategy for fighting these threats."[1] The actions laid out in the Road Map include numerous tasks for all stakeholders – including private sector players in the communications, Internet, and information technology industries – which "could dramatically reduce the threat of botnets and similar attacks consistent with Administration priorities as set forth in the **National Cyber Strategy**."[2]

The *Botnet Report* was called for in the President's May 2017 Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," and sets out 24 actions for public- and private-sector stakeholders to take on. A Wiley Rein LLP summary of the *Report* can be found **here**.

WHAT'S IN THE ROAD MAP?

The newly released Road Map is broken into five "Lines of Effort," including:

1. Internet of Things
2. Enterprise
3. Infrastructure
4. Technology Development and Transition
5. Awareness and Education

Each line of effort relates directly to actions called for in the *Botnet Report* and lays out subtasks and potential timelines for completion. "Some tasks will be the direct responsibility of the federal government, while others are specific to the private sector."[3] Further, "where applicable, [the Road Map] identifies existing private-sector leaders or governance structures for the relevant tasks."[4]

The Road Map states that while government has the power to convene stakeholders, "achieving the outcomes set forth in the *Botnet Report* will require industry and civil society engagement from across the ecosystem. The identified tasks and associated information should be seen as non-binding and flexible to accommodate changes in the digital ecosystem over time."[5] The Road Map states "the U.S. government values innovation, and expects the market to determine the most expeditious solutions to the identified concerns."[6]

LINES OF EFFORT AND WORKSTREAMS INVOLVING INDUSTRY

As stated above, the Road Map is organized into five lines of effort. Within each line, the Departments identify primary "workstreams" which include multiple "tasks" for various actors. Below, we provide high-level summaries of the major lines of effort and the workstreams involving industry contributors.

1. IoT: Raising the Bar for IoT Security

The first workstream in the IoT line is ***Developing Robust Markets for***

continued on page 4

continued from page 3

Trustworthy IoT Devices "that offer security capabilities for three sectors: consumers/ home users, industrial users, and the federal government."[7]

In order to do this, the first goal sets out to *Define a Core Security Capability Baseline* "that could be supported by the full range of assessment schemes. At a minimum, the capability baseline would address device and data security. [The National Institute of Standards and Technology (NIST)] will publish the consensus baseline as a NIST white paper or Interagency Report (NISTIR) for reference and use in future tasks."[8]

Under the three-sector approach, each of the following goals apply to a specific operational environment. The second goal is *Establishing a Robust Market for Trustworthy Consumer/ Home IoT Devices*.[9] This includes such tasks as: Developing Consumer/Home IoT Security Baseline; Establishing or Supporting Assessment Programs for Consumer/Home IoT Devices; and Exploring Labeling for Consumer/Home IoT.

The third goal is *Establishing a Robust Market for Trustworthy Industrial IoT Devices*.[10] The tasks mirror those in the Consumer/Home environment, but also include Promoting Adoption of an Assessment Regime by Critical Infrastructure.

The last goal follows the same pattern for *Federal IoT Devices,*[11] but notably, sets out that "[t]o encourage acquisition and deployment of conforming devices, federal procurement regulations [will be] established that reference the federal baseline."[12] Tasks include: Identifying Federal IoT Security Requirements; Specifying a Federal IoT Security Capability Baseline; and Establishing Federal IoT Procurement Regulations. The Road Map notes that a series of meetings will be convened with stakeholders.

The second IoT workstream relates to ***Adoption and Sustainability for IoT Security***, focusing "on the development of the global ecosystem for IoT devices[.]"[13] These tasks concentrate "on collaboration between cybersecurity and operational technology communities, and international policy advocacy, harmonization, and standards."[14]

The first goal in this workstream is *Enabling Risk Management Approach to IoT Security*. The Road Map's goal is to publish NISTIR 8228, "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks," to support risk management approaches to IoT security. Further tasks include Publishing Best Practices for IoT Device Manufacturers; Aligning Usability and Manageability with Customer Abilities; among others.

The next goal is *Establishing Globally Relevant IoT Standards*. "The Botnet Report noted that 'U.S. government and industry should jointly engage with developers of industry-led, voluntary international standards and specifications to establish globally relevant standards.' This series of tasks encourages U.S. government and industry to jointly pursue international standards consistent with the capability baselines developed in the previous workstream."[15] Tasks include identifying incentives for IoT adoption of security standards.

2. Enterprise

The Enterprise line of effort has four complementary workstreams: Cybersecurity

continued on page 5

Framework (CSF) profiles for mitigation and protection, migration to advanced enterprise network architectures, federal adoption of enterprise best practices, and operational technology.

This first workstream is ***Implementing CSFs For Mitigating Distributed Denial of Service (DDoS) Threats and Combatting Botnets***. Industry efforts have been led by the Cybersecurity Coalition, which published a framework core.[16] Efforts will revolve around working to develop industry consensus for CSF Profiles for DDoS and Botnet Threat Mitigation. After completion of the industry-led profiles, the federal government will tailor these profiles for the federal environment.

The second workstream is ***Advancing Enterprise Network Architectures***. "Enterprises should migrate to network architectures that facilitate detection, disruption, and mitigation of automated, distributed threats. They should also consider how their own networks put others at risk."[17] Tasks directly involve network operators and service providers and will include: Enhancing and Evolving Best Practices on Enterprise Network Traffic Management; Promoting Enterprise Network Architectures that Mitigate Risks of Automated, Distributed Threats; Accelerating and Domestic Availability of and Transition to IPv6 Internet Services and Networks; Establishing Requirements for Zero Trust Networking (ZTN); and Identifying Best Practices for IoT Network Management; and others.[18]

The next workstream under the Enterprise line of effort is ***Federal Adoption of Enterprise Best Practices***. This includes activities the government can take to reduce automated, distributed threats, such as implementing egress filtering to prevent network address spoofing. "In this series of tasks, the federal government performs activities to ensure that these best practices are properly reflected in federal agency policies, standards, guidelines, and oversight."[19]

Related to the ***Operational Technology*** workstream, tasks will focus on "clos[ing] gaps in understanding between the cybersecurity and operational technology (OT) communities."[20] Tasks include: Expanding Collaboration between Cyber and OT communities; Expanding OT-Cybersecurity Information Sharing; and Expanding Federal Government Involvement.

3. Infrastructure

The Infrastructure effort "focuses on actions that will require coordination across the vast diversity of digital ecosystem players, or that impact the core functional capabilities of the global digital infrastructure."[21] It has four workstreams: improvements to routing security, information sharing in practice, information sharing protocols, and research and development.

The first workstream of ***Improving Routing Security*** notes that "the state of routing security on the Internet falls far below what can be achieved with both common and newer tools and practices. This series of tasks advances deployment of longstanding anti-spoofing technologies and newer technologies to protect against route hijacks and leaks."[22] One task is to Develop Security Requirements for Internet Services, and requires publishing NIST Special Publication 800-189, "Secure Inter-Domain Traffic Exchange: BGP Robustness

continued on page 6

continued from page 5

and DDoS Mitigation." Additional tasks include: Removing Legal and Policy Barriers to Resource Public Key Infrastructure (RPKI) Adoption; Federal Adoption of RPKI; Extending Adoption and Awareness of Anti-Spoofing Mechanisms; and others.

The second workstream relates to improved ***Information Sharing in Practice***. The Road Map's tasks are geared towards "extending information sharing to smaller ISPs and foreign network providers, and ensuring that law enforcement is alerted at the earliest possible stage, while respecting privacy guidelines and regulations."[23] Tasks revolve around: Increasing Smaller ISPs' Access to Industry-Shared Threat Information; Expanding Information Sharing Agreements; Sharing Timely and Actionable Information with Law Enforcement; Improving U.S Government Information Sharing with Industry; and Enhancing the Accuracy of Security-Critical Data Resources.

Another workstream focuses on standardization of ***Information-Sharing Protocols*** to increase speed and permit automated response.[24] Tasks include: Supporting Information Sharing Automation; Supporting Collaborative Incident Response; and Establishing International Standards to Facilitate Information Sharing; among others.

The final workstream in the Infrastructure line of effort is bolstering ***Research and Development***. Tasks include: Incorporating Infrastructure Best Practices into the NIST Cybersecurity Framework and Disrupting the Attacker Ecosystem Through Transparency and Traceability.[25]

4. Technology Development and Transition

The line of effort for Technology Development and Transition has three workstreams: establishing a secure software marketplace, international coordination, and research and development.

Under the workstream of ***Establishing a Secure Software Marketplace***, "[t]asks establish widely accepted guidelines for secure software development, increase the efficiency and effectiveness of tools for secure software development to increase return on investment, and showcase these advances in government sponsored technology forums."[26] Specific efforts include: Establishing Secure Software Development Lifecycle Guidelines; Developing Guidelines for Software Component Transparency; Filling Gaps in Software Development Tools; Showcasing Advances in Secure Coding Practices and Sharing Information about Security Risks; Requiring Secure Development for Government Off-the-Shelf (GOTS) Software; Developing Best Practices for End-of-Life Software; and others.

The next workstream is ***International Coordination***, which includes: Improving Existing U.S. Government Coordination on International Standards; Optimizing Industry-USG Standards Coordination; Promoting International Adoption of Best Practices Through Bilateral and Multilateral International Engagement; Promoting Awareness and Adoption of Specific Established Tools, Protocols, and Best Practices at a Global Scale; and Promoting Best Practices for DNS Internationally. While some of these efforts will be led by the government, industry is also expected to engage.

The third workstream relates to ***Research and Development***. The Road Map highlights that, "Industry-led research activities are

continued on page 7

continued from page 6

needed to develop and deploy innovative technologies. As a key source of funding for basic research in cybersecurity, the federal government should support this action through targeted funding and collaborative technology transition activities."[27] Tasks include: Accelerating Federally Funded R&D for Mitigating Distributed Threats; Expediting Development and Deployment of Innovative Technologies for Prevention and Mitigation of Distributed Threats; Increasing Accountability in Traffic Management; Accelerating Industry R&D for Mitigating Distributed Threats; Prioritizing Technology Transfer; and Promoting Best Practices.

5. Awareness and Education

The final line of effort is aimed at promoting consumer confidence and educating the workforce.

The first workstream is to ***Promote Consumer Confidence***. The Road Map states that, "[c]onsumers' lack of confidence in the security of IoT devices may be hindering IoT adoption. This series of tasks focuses on building consumer confidence to allow consumers to identify products that meet their needs, adhere to vendors' security claims, and that offer real protection by applying commercially available cybersecurity technologies."[28] Tasks include: Promoting Appropriate Product Deployment; Deterring Illegal Market Practices; and Mitigating IoT-based DDoS.

The second workstream is ***Educating the Workforce***. The Road Map outlines that "Product designers are deeply steeped in traditional risks associated with their products, but are often unaware of the new risks that can be introduced when the products are connected to the network. This series of tasks focuses on educating the existing and emerging workforce, regardless of engineering discipline, on basic cybersecurity."[29] Tasks are: Preparing the Programming Workforce; Preparing the Engineering Workforce; Promoting the National Initiative for Cybersecurity Education (NICE) Framework; and Establishing Cybersecurity Educational Program for Engineers.

TRACKING STAKEHOLDER PROGRESS AND NEXT STEPS

In an accompanying announcement, DOC's National Telecommunications and Information Administration outlines that "[t]his is just a starting point and the road map will evolve to address the rapid changes in digital technologies and the threat environment. The departments will track progress through regular stakeholder meetings as well as a workshop. In addition, the departments will provide a status update to the President that reviews progress, tracks the impact of the road map, reassesses the botnet threat, and sets further priorities."[30]

The DOC and DHS "will develop a 365-day status update for the President, due [November 29, 2019]." This update will cover:

1. Progress the community as a whole is making against the road map;
2. The impacts of those road map activities;
3. A reassessment of the threat of automated, distributed attacks, including whether the threat is increasing or decreasing, and any known reasons for such a change; and
4. What activities should be prioritized in the coming year.[31]

continued on page 8

continued from page 7

The Departments seek feedback on all elements of Road Map tasks, particularly the identification of contributing partners for specific actions and proposed timelines. Comments on the Road Map may be submitted to **Counter_Botnet@list.commerce.gov**. ■

For more information, please contact:

Michael L. Diakiwski
202.719.7031
mdiakiwski@wileyrein.com

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Kathleen E. Scott
202.719.7577
kscott@wileyrein.com

Endnotes

[1] *See* **https://www.ntia.doc.gov/blog/2018/road-map-building-more-resilient-internet**

[2] Departments of Commerce and Homeland Security, *A Road Map Toward Resilience Against Botnets*, 3 (Nov. 29, 2018) (Road Map).

[3] Road Map at 3.

[4] Road Map at 4.

[5] Road Map at 3.

[6] Road Map at 4.

[7] Road Map at 5.

[8] Road Map at 5.

[9] Road Map at 6-7.

[10] Road Map at 7-8.

[11] Road Map at 8-9.

[12] Road Map at 8.

[13] Road Map at 9.

[14] Road Map at 9.

[15] Road Map at 10.

[16] *See* **https://docs.wixstatic.com/ugd/86b770_df02de6fc3ae422ea492200018c34217.pdf**.

[17] Road Map at 12.

[18] Road Map 12-14.

[19] Road Map at 14.

[20] Road Map at 15.

[21] Road Map at 16.

[22] Road Map at 16.

[23] Road Map at 18.

[24] Road Map at 19.

[25] Road Map at 20.

[26] Road Map at 21.

[27] Road Map at 24.

[28] Road Map at 25.

[29] Road Map at 26.

[30] *See* **https://www.ntia.doc.gov/blog/2018/road-map-building-more-resilient-internet**.

[31] Road Map at 4.

continued from page 1

more research. This kind of feedback will be important as the agency continues its "Hearings on Competition and Consumer Protection in the 21st Century" to further explore consumer privacy issues in the coming year.

The nature and extent of any harm from the disclosure of private information matters greatly to the FTC. In order to challenge a practice as "unfair," the FTC must show that the challenged practice causes or is likely to cause substantial injury that is not reasonably avoidable by consumers, and that the injury is not outweighed by countervailing benefits to consumers or competition.[1] And even in weighing whether to bring an enforcement action under a deception theory, or in determining whether and what kind of policy recommendations to make, the nature and severity of the harm are important. Staff weigh such a determination in exercising prosecutorial discretion and in evaluating whether the benefits of FTC action outweigh the costs. Robust, empirical studies to quantify certain kinds of harm from the disclosure of information can carry great weight in FTC decision-making regarding enforcement and policy development.

The FTC has recently sought out more information on what kinds of harms might result from disclosure of different kinds of consumer information. In December 2017, the FTC held a workshop on "informational injuries," which staff explained as injuries "that consumers may suffer from privacy and security incidents, such as data breaches or unauthorized disclosure of data."[2] In October 2018, staff from the Bureau of Consumer Protection and Bureau of Economics released a staff perspective paper summarizing key takeaways from the workshop.

The staff perspective first provides examples of different kinds of informational injury, including:

- **Doxing.** Doxing involves the deliberate and targeted release of an individual's private information, often with the intent of harassment or injury. The information can be used for social engineering attempts to trick individuals into revealing more private information, extortion attempts, and other sorts of harassment that can result in threats of physical harm.[3]
- **Disclosure of private information.** Disclosure of personal information that an individual wishes to keep private – such as medical information – may potentially affect employment possibilities or negatively affect relationships with friends and family.[4]
- **Erosion of trust.** Some participants suggested that unanticipated disclosures may "erode consumers' trust in the ability of businesses to protect their data," and thereby undermine benefits provided by online businesses.[5]
- **Medical identity theft.** Use of a consumer's identity to obtain health care services can not only potentially cause financial harm, but may also result in a consumer's medical file containing inaccurate information, which could adversely affect the individual's safety or treatment.[6]

Second, staff notes that these injuries must be balanced against the potential benefits to consumers of collecting certain kinds of

continued on page 10

FTC Focuses on Potential Types of 'Informational Injuries' as It Re-Examines Approach to Consumer Privacy

continued from page 9

data, including enabling an ad-supported Internet model in which consumers pay little or no fees; preventing fraud and allowing for more robust identity verification; allowing for location-based map services; and allowing for the customization of services.[7]

Third, staff notes that stakeholders continue to debate the potential benefits and costs of government action. Without resolving the debate, staff notes that participants "appeared to coalesce around several factors that governments should consider."[8] These include:

- **Sensitivity of the data at issue.** Social Security numbers, financial information, and health information are more sensitive than other kinds of information and weigh more heavily toward protection from disclosure.
- **How the information will be used.** On this, staff notes that "[i]nternal, expected uses would not generate the same level of concern as unexpected uses for some other purpose."
- **Whether the information is anonymized or identifiable.** Sharing anonymized data could potentially be beneficial for research purposes.[9]

Fourth, staff discusses the current state of research regarding the value consumers assign to the privacy of certain information. Staff describes the phenomenon of the "privacy paradox," in which consumers state in surveys that they care about privacy, but then act in ways inconsistent with their stated preference – which has generated a range of potential explanations.[10] Without resolving the competing explanations for the current studies, staff calls for more research to illuminate these issues, including:

- Further consumer surveys of what consumers value in protecting data, including studies that might attempt to quantify how much consumers value certain privacy protections.
- Empirical studies on the efficacy of data protection measures, such as credit card chips and multi-factor authentication, to inform determination of how effective certain measures can be.
- Studies to track downstream injury from information disclosure, such as attempting to link specific data breaches to a specific harm such as identity theft.[11]

FTC staff's recent comment to the NTIA, in response to a Request for Comment on developing the Administration's privacy approach, echoes this framework of weighing injuries from information disclosure in assessing the costs and benefits of government action, including the potential effects on pro-consumer innovative technologies.[12] In particular, the comment provides examples of privacy-related harms that fall into at least four categories, including financial injury, physical injury (such as risks of stalking), reputational injury, and unwarranted intrusions (including both intrusions into the sanctity of people's homes and intimate lives as well as unwanted commercial intrusions). And it cites to numerous examples of how the use of consumer data can improve consumers' lives, including improved consumer fraud detection, free or substantially discounted services, and safer homes, among others.[13]

The FTC is continuing to re-assess its approach to privacy, including taking a

continued on page 11

continued from page 10

closer look at balancing the costs and benefits of government action, and 2019 will provide more opportunity for comment. On February 12-13, the Commission will host a two-day hearing on consumer privacy, which it has billed as "the first comprehensive re-examination of the FTC's approach to consumer privacy since 2012."[14] Many of the preliminary questions for consideration deal with how to define and quantify harm from disclosures of consumer information.[15] The deadline for submitting comments is March 13, 2019, and as Wiley Rein **has previously noted**, FTC officials have encouraged stakeholders to submit comments with tangible, data-driven analysis on the topics of privacy-related harm. Expect the FTC to continue focusing on injury-related questions as it continues its evaluation of privacy law and policy. ■

For more information, please contact:

Duane C. Pozza
202.719.4533
dpozza@wileyrein.com

Endnotes

[1] 15 U.S.C. §§ 45(a), 45(n).

[2] *See* FTC Staff, *FTC Informational Injury Workshop: BE and BCP Staff Perspective*, October 2018, available at **https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf** ("Staff Perspective"), at 1. The workshop homepage is at **https://www.ftc.gov/news-events/events-calendar/2017/12/informational-injury-workshop**.

[3] Staff Perspective at 2.

[4] *Id*.

[5] *Id*. at 3.

[6] *Id*. at 1-2.

[7] *Id*. at 3.

[8] *Id*. at 4.

[9] *Id*. A related topic on which there was less agreement was whether the government should consider a greater risk of injury as part of its injury calculus. The workshop participants' mixed views on this issue is reflective of recent FTC history. In overturning an FTC Administrative Law Judge's ruling in favor of LabMD in a case that involved the disclosure of large volume of consumer data without an evidentiary record of actual misuse, the Commission, under then-Chairwoman Ramirez, articulated a theory that harm is present if the magnitude of potential injury is large even if the likelihood of injury is low. *See In re LabMD*, FTC Docket No. 9357, at 10, 21 (2016), available at **https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf**. In overturning the Commission's *LabMD* decision, the Eleventh Circuit did not reach the question of whether this is the appropriate standard. It remains to be seen whether the FTC under Chairman Simons will explicitly adopt this standard.

[10] *Id*. at 5-6.

[11] *Id*. at 6-7.

[12] Comment of FTC Staff, *In re Developing the Administration's Approach to Consumer Privacy*, NTIA Docket No. 180821780-8780-01 (Nov. 9. 2018), available at **https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf**.

[13] *Id*. at 8-11.

[14] *See* FTC Press Release, "FTC Announces Sessions on Consumer Privacy and Data Security as Part of its Hearings on Competition and Consumer Protection in the 21st Century," October 26, 2018, available at **https://www.ftc.gov/news-events/press-releases/2018/10/ftc-announces-sessions-consumer-privacy-data-security-part-its**.

[15] The hearing page is available at **https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-february-2019**. Looking further out, the FTC will host its fourth annual PrivacyCon on June 27, 2019; the agency is seeking research presentations on consumer privacy and security issues, including the quantification of costs and benefits to consumers of keeping data about them private. More information is available at **https://www.ftc.gov/news-events/events-calendar/privacycon-2019**.

The First Amendment Right to Political Privacy
Chapter 3 — Red Monday, Paul Sweezy, and the Frankfurter Concurrence

By Lee E. Goodman

Chapter 1 recounted the plight of the "Hollywood Ten" communists, who went to prison and lost their careers rather than disclose the names of fellow communists to the House Committee on Un-American Activities (HUAC) in 1947. Their fate was decided by the U.S. Court of Appeals for the District of Columbia, and the Supreme Court was unwilling to wade into the Red Scare. **Chapter 2** covered the First Amendment protection the U.S. Court of Appeals for the District of Columbia and the Supreme Court afforded, a few years later, to the conservative Committee on Constitutional Government and its political efforts to thwart the New Deal. This Chapter 3 recounts how the Supreme Court slowly began to intervene in the Red Scare, culminating with a significant concurring opinion by Justice Felix Frankfurter in the case of Marxist political activist Paul Sweezy one decade after the Hollywood Ten appeared before the HUAC.

No Judicial Relief from the Red Scare – In Calmer Times?

By 1950, the Red Scare was in full bloom and enjoyed general public favor. Many of the Hollywood Ten were serving prison sentences. Both houses of Congress, the Executive branch, and states were actively investigating former or current communists in various settings, exposing them, and punishing them. The First Amendment was deemed a weak defense in light of the Hollywood Ten outcome. Some subpoena recipients invoked their Fifth Amendment rights to avoid inquiry, but that entailed implicating oneself in a criminal act, so it was imperfect. Many just named names and cooperated in order to avoid punishment.

Dozens of court cases were underway challenging the various governmental actions. Judicial conservatives on the Supreme Court were not impressed by the constitutional claims and either denied certiorari or affirmed lower court decisions, ruling against communists in various contexts.[1] The prevailing view was that the government had a right of self-preservation and Congress was pursuing the national security interest justly by rooting out communists. In the words of one communist defense attorney of the day, "The courts were of no help whatsoever."[2]

Congress had enacted the Smith Act in 1940, which made it a crime to advocate the overthrow of the U.S. government by force or violence.[3] Over a hundred American citizens were indicted for alleged violations of the Smith Act.[4] In 1948, the conviction of Eugene Dennis, General Secretary of the Communist Party USA, was affirmed by the U.S. Court of Appeals for the Second Circuit.[5] The Supreme Court granted certiorari for the purpose of deciding if the Smith Act violated the First Amendment.

In a 6-2 opinion, issued in 1951, the Supreme Court unremarkably affirmed the convictions and found no First Amendment violation.[6] Majority opinions ranged from the important governmental interest in self-preservation to relatively carte blanche deference to the Legislative branch. As in the Hollywood Ten case, two Justices

continued on page 13

continued from page 12

dissented, William O. Douglas and Hugo Black, the former Senator and KKK member who was an absolutist defender of First Amendment rights. Both Justices recognized the First Amendment right of communists to associate and advocate their ideas short of organizing overthrow of the government. Justice Douglas observed simply that the party leaders taught communist economic ideology, but never did anything to incite actual armed overthrow of the government. In one of the more pertinent observations of the time, Justice Black prophesized:

> There is hope, however, that in calmer times, when present pressures, passions and fears subside, this or some later Court will restore the First Amendment liberties to the high preferred place where they belong in a free society.[7]

Calmer Times Ahead – First Amendment Jurisprudence Evolves

By the early 1950s, the HUAC had resumed its investigations into communists soon after the Supreme Court denied certiorari in the Hollywood Ten case in 1950, under the leadership of Georgia Democrat John Stephens Wood. Meanwhile, in the Senate, a first-term Senator from Wisconsin named Joseph McCarthy focused investigations on Soviet spies in the State Department and the Defense Department from his perch as chairman of the Senate Permanent Subcommittee on Investigations. The nation was gripped by televised hearings and headlines about communist spies and other subversives.

Gradually, however, public and political support for communist hunting waned. McCarthy had taken on powerful institutional opponents in two Presidents, Truman and Eisenhower, neither of whom appreciated his embarrassing charges that their administrations did too little to root out Soviet spies. Increasingly, his Senate colleagues seized on reckless tactics to discredit valid claims and marginalize the Senator. In June 1954, McCarthy had perhaps bitten off more than he could chew in taking on the U.S. Army's recalcitrant measures to remove disloyal spies and fix lax security at the Army base in Monmouth, New Jersey – culminating in ethics counter-charges and a sharp exchange with Army attorney Joseph Welch who famously turned an audience against McCarthy with the line "Until this moment, Senator, I think I never really gauged your cruelty or your recklessness," and after further verbal jousting, "Let us not assassinate this lad further, Senator. You have done enough. Have you no sense of decency?" Some historians have credited that televised retort as the end of Joe McCarthy's career, regardless of the merits of his charges.

Shortly thereafter, on December 2, 1954, the Senate voted to "condemn" McCarthy for abusive conduct by a vote of 67-22.[8] After Democrats took over the Senate, McCarthy no longer held a committee chairmanship as a platform for his investigations. In May 1957, McCarthy died at the age of 48. Ever since, his political legacy – often referred to as "McCarthyism" – has been painted by American liberals, as well as some conservatives, as the ruin of reputations, livelihoods, and progressive causes through unfair intrusions into private realms of political belief and associations, public disclosure, and ridicule.[9]

continued on page 14

Chapter 3 — Red Monday, Paul Sweezy, and the Frankfurter Concurrence

continued from page 13

Something else was happening in the mid-1950s. Four new Justices were appointed to the Supreme Court between 1950, when the Court denied certiorari to the Hollywood Ten, and 1957. The departing Justices were judicial conservatives Stanley Reed, Robert Jackson, Fred Vinson, and Sherman Minton. The new Justices were Earl Warren, William Brennan, Charles Whittaker, and John Harlan. They joined the two First Amendment libertarians – Hugo Black and William O. Douglas – along with Felix Frankfurter, Harold Burton, and Tom Clark.

This was the situation in 1957 when the Supreme Court finally took up several challenges to Red Scare investigations at various levels of government.

The Case of Paul Sweezy

Investigations of communists were not limited to the federal government and Congress. Many states decided they too had a role to play in protecting the United States from communist subversion. States adopted a variety of policies to purify state governments, public schools, and universities, state bars, and society at large from communists.

New Hampshire was such a state. It had adopted a law in 1951 authorizing the state attorney general to investigate, with subpoena power, any citizen suspected of being a "subversive person" – defined to mean any person who so much as attempted or encouraged "any act intended to overthrow, destroy or alter, or to assist in the overthrow, destruction or alteration of, the constitutional form of the government of the United States, or of the state of New Hampshire, or any political subdivision of either of them, by force, or violence."[10]

The statute declared "subversive persons" to be ineligible for employment by the state government and required all public employees to make sworn statements they were not "subversive persons." The law declared "subversive organizations" to be unlawful and dissolved.

In January 1954, as Senator McCarthy was preparing to launch public hearings into security leaks at the Army's facility in Monmouth, the New Hampshire attorney general, Louis Wyman, issued subpoenas to Marxist economist Paul Sweezy as a suspected "subversive person."

Paul Marlor Sweezy (1910-2004) was a committed Marxist economist. According to one biographer, "Paul M. Sweezy, referred to by *The Wall Street Journal* in 1972 as 'the 'dean' of radical economists,' was, in the words of John Kenneth Galbraith, 'the most noted American Marxist scholar' of the second half of the twentieth century."[11] The son of a prominent New York banker, he was educated at Exeter and Harvard, ultimately receiving his Ph.D. in economics. He had been an avid New Dealer, working in various posts in the Roosevelt Administration. He later served in the U.S. Army during World War II as an officer in the Army's Office of Strategic Services, where he studied the European economy. After the war, he settled in Wilton, New Hampshire, and married Nancy Adams and had three children. He was an active writer and lecturer. He was politically active too, supporting the presidential candidacy of Progressive Party nominee Henry Wallace (former Vice President of the United States from 1941-1945) in 1948 and founding the Progressive Party of New Hampshire. The Progressive

continued on page 15

Chapter 3 — Red Monday, Paul Sweezy, and the Frankfurter Concurrence

continued from page 14

Party was a meeting point for many American communists. In addition to writing several books and monographs on Marxist economic theory,[12] Sweezy founded the Marxian economic journal *Monthly Review* in 1949, a journal still published today.[13]

Sweezy must have appeared to the New Hampshire attorney general to be a shiny object in an otherwise sleepy state. At a time when socialist economic thought was equated in broad brushes with communist overthrow of the American democratic system, Attorney General Wyman bore down on Sweezy as the embodiment of a "subversive person." Wyman subpoenaed Sweezy to testify on two separate occasions, and Sweezy complied and testified at length for two full days, January 5, 1954 and June 3, 1954.

However, before he testified, Sweezy prefaced his first sitting with a statement of principle. He defended the right of political conscience against government inquiry:

> [T]here are those who are not Communists and do not believe they are in danger of being prosecuted, but who yet deeply disapprove of the purposes and methods of these investigations…. Our reasons for opposing these investigations are not captious or trivial. They have deep roots in principle and conscience…. Whatever their official purpose, these investigations always end up by inquiring into the politics, ideas, and beliefs of people who hold what are, for the time being, unpopular views.[14]

Seeking to eliminate the Attorney General's statutory predicate for intruding into his political beliefs, he denied ever advocating the overthrow of the United States government by force or violence, or knowing anyone else who ever had:

> I have studied the subversive activities act of 1951 with care, and I am glad to volunteer the information that I have absolutely no knowledge of any violations of any of its provisions; further, that I have no knowledge of subversive persons presently located within the state.[15]

Having inoculated himself, and having laid a foundation for his subsequent constitutional challenge to contempt proceedings, Sweezy qualified the extent of his intended cooperation:

> I shall respectfully decline to answer questions concerning ideas, beliefs, and associations which could not possibly be pertinent to the matter here under inquiry and/or which seem to me to invade the freedoms guaranteed by the First Amendment to the United States Constitution.[16]

Sweezy then appeared and testified for two full days of questioning. He answered questions about his own political activities, his military service, his ideology (which was fully public in numerous writings), which he characterized as "classical Marxist," and he denied that he had ever been a member of the Communist Party.[17]

Critically, however, Sweezy declined to answer several targeted questions. First, he declined to disclose the names of other members of the Progressive Party or a predecessor organization, Progressive Citizens of America, both considered congregating places for American communists.[18] Second, he declined to

continued on page 16

continued from page 15

answer the question "Do you believe in Communism?"[19] And third, Sweezy refused to discuss the substance of a lecture he delivered at the University of New Hampshire.[20]

For his refusals to answer these questions, Attorney General Wyman filed a petition in state court seeking to compel Sweezy to answer. The state court ruled the questions pertinent to the Attorney General's statutory charge and inquiry, and propounded the questions directly to Sweezy. When Sweezy persisted in refusing to answer, the state court ruled Sweezy to be in contempt and ordered him to be confined in jail until he purged himself of contempt.[21]

Sweezy appealed, first to the New Hampshire Supreme Court, which upheld Sweezy's conviction for refusing to disclose members of the Progressive Party.[22] Sweezy then appealed to the U.S. Supreme Court. The Supreme Court, which had denied certiorari to the Hollywood Ten a decade earlier, granted review to Sweezy.[23]

"Red Monday" – June 17, 1957

Monday, June 17, 1957, marked a turning point in the Red Scare. That day, the Supreme Court issued four decisions curtailing government efforts to root out communists.

In *Yates v. United States*,[24] the Court overturned the conviction of Oleta O'Connor Yates, a Communist Party leader in California for many years, under the Smith Act on the narrow basis of confusing and inadequate jury instructions.

In *Service v. Dulles*,[25] the Court unanimously ruled that the State Department improperly terminated John Service, widely considered to be a pro-communist foreign service officer who shared agency secrets with pro-communist publications, from employment on technical procedural grounds.

Two decisions significantly curtailed government interrogations of communists. In *Watkins v. United States*,[26] the Court clipped the wings of the House Un-American Activities Committee (HUAC), ruling that Congress' authorizing resolution was overly vague and the committee's explanation to labor leader John Watkins was "woefully inadequate to convey sufficient information as to the pertinency of the questions to the subject under inquiry."[27] In a significant concurring opinion, Justice Frankfurter, a judicial conservative, opined that the HUAC's subpoena failed to provide Watkins "awareness of the pertinency of the information that he has denied to Congress."[28] Watkins, unlike the Hollywood Ten a decade earlier, had answered almost all of the HUAC's questions about himself, but, like Sweezy, had declined to "answer any questions with respect to others with whom I associated in the past."[29] He continued, "I do not believe that any law in this country requires me to testify about persons who may in the past have been Communist Party members or otherwise engaged in Communist Party activity but who to my best knowledge and belief have long since removed themselves from the Communist movement…. [U]ntil and unless a court of law so holds and directs me to answer, I most firmly refuse to discuss the political activities of my past associates."[30]

Finally, in *Sweezy v. New Hampshire*, the Court overturned Paul Sweezy's contempt conviction on the grounds that the Attorney

continued on page 17

Chapter 3 — Red Monday, Paul Sweezy, and the Frankfurter Concurrence

continued from page 16

General of New Hampshire exceeded his authority under the New Hampshire Subservice Activities Act of 1951 – as well as First Amendment grounds.[31]

J. Edgar Hoover was incensed. According to legal scholar Arthur Sabin, Hoover prided himself in protecting the nation from those he considered dangerous political dissenters. "Then came June 17, 1957, a day he called 'Red Monday' – not because of the red-hot weather, but because, as he saw it, that day the United States Supreme Court handed down four decisions favoring the 'Reds.'"[32] Hoover publicly denounced the Warren Court for weakening the United States' defenses to foreign influence and subversion.

Sweezy v. New Hampshire – The Supreme Court Weighs In

Sweezy was the most important decision for First Amendment jurisprudence. The vote was 6-2 for reversal. Chief Justice Warren, writing for the four-Justice majority, observed that the New Hampshire Attorney General's subpoenas encroached upon constitutional rights:

> There is no doubt that legislative investigations, whether on a federal or state level, are capable of encroaching upon the constitutional liberties of individuals. It is particularly important that the exercise of the power of compulsory process be carefully circumscribed when the investigative process tends to impinge upon such highly sensitive areas as freedom of speech or press, freedom of political association, and freedom of communication of ideas, particularly in the academic community.[33]

The Court continued:

> Merely to summon a witness and compel him, against his will, to disclose the nature of his past expressions and associations is a measure of governmental interference in these matters. These are rights which are safeguarded by the Bill of Rights and the Fourteenth Amendment. We believe that there unquestionably was an invasion of petitioner's liberties in the areas of academic freedom and political expression – areas in which government should be extremely reticent to tread.[34]

Yet, after further elaborating on the "political freedom of the individual" and the concomitant rights of associations of adherents, as well as the right of dissent (perhaps ideas insisted upon by Justices Black and Douglas), the majority opinion held that the New Hampshire Attorney General acted ultra vires, beyond the scope of the authority clearly prescribed in the New Hampshire legislature's authorizing statute. "As a result," the Court observed, "neither we nor the state courts have any assurance that the questions petitioner refused to answer fall into a category of matters upon which the legislature wanted to be informed when it initiated this inquiry."[35] The Court went on to reason that without a clear writ, the Court could not adequately assess the state interest. The Court concluded that the "lack of any indications that the legislature wanted the information the Attorney General attempted to elicit from [Sweezy] must be treated as the absence of authority. It follows that the use of the contempt power, notwithstanding the interference with

continued on page 18

continued from page17

constitutional rights, was not in accordance with the due process requirements of the Fourteenth Amendment."[36]

Thus, in the final analysis, the majority holding was narrow and limited in scope, similar to the *Watkins* decision on pertinence. The First Amendment rights were implicated but not decisively violated.

The Frankfurter Concurrence – The First Amendment Protects Political Privacy

Justice Frankfurter, joined by Justice Harlan, had difficulty joining Chief Justice Warren's broad attack at state legislative and prosecutorial authority.[37] Frankfurter reasoned that the New Hampshire Supreme Court definitively had decided that the Attorney General acted well within the legislative authority granted to him by state statute, so the United States Supreme Court was in no position to second-guess the state court or the Attorney General's authority. Therefore, Frankfurter addressed the First Amendment (as applied to the state through the Fourteenth Amendment) challenge head-on. He concluded that the Attorney General's inquisition, and specifically the questions requiring Sweezy to disclose the names of Progressive Party members, violated the First Amendment right of "political privacy." Based solely upon the First Amendment, he decided to reverse Sweezy's contempt conviction. The language written by Frankfurter was particularly declarative of the right to "political privacy" against government inquisition:

> [T]he inviolability of privacy belonging to a citizen's political loyalties has so overwhelming an importance to the well-being of our kind of society that it cannot be constitutionally encroached upon on the basis of so meagre a countervailing interest of the State as may be argumentatively found in the remote, shadowy threat to the security of New Hampshire allegedly presented in the origins and contributing elements of the Progressive Party and in [Sweezy's] relations to these. In the political realm, as in the academic, thought and action are presumptively immune from inquisition by political authority.[38]

Frankfurter opined that "the right of a citizen to political privacy" wholly outweighed New Hampshire's interest in "self-protection."[39] This was the clearest statement yet on the Supreme Court that the First Amendment protects political privacy against the government's demand for disclosure of political associations.

Ironically, it was Justice Frankfurter, the conscientious judicial conservative, who carefully avoided a head-on First Amendment ruling in *United States v. Rumely* five years earlier, providing the full-throated First Amendment rebuke to communist inquisition, while First Amendment libertarians Justice Black and Justice Douglas, who issued a broad First Amendment concurrence in *Rumely*, joined the more restrained main holding authored by Chief Justice Warren. But significantly, Frankfurter and Harlan had now signed on fully to the First Amendment right of all citizens to political privacy.

Aftermath

The Red Monday decisions marked a critical point of political and law enforcement inflection. According to legal scholar Sabin:

> In sum, the Justice Department and the FBI recognized the Red

continued on page 19

continued from page 18

> Monday decisions of June 17, 1957 as confirmation of a changed majority position on the Supreme Court on Red Scare issues. The *Yates* decision of Red Monday meant that further Smith Act prosecutions of communists would be a waste of time, money, and effort…. What had begun in 1948 with the indictment of the top eleven Communist Party members pragmatically ended in 1957. The Supreme Court gave a green light to criminal charges under the Smith Act with the *Dennis* decision in 1951; in 1957, the light turned red.[40]

Although Smith Act prosecutions would be curtailed after Red Monday, the Supreme Court would nevertheless later retreat, in subsequent cases, from its defense of communists under government investigation generally.[41] The Court's retreat, and particularly Frankfurter's reticence, came in response to withering political attack from J. Edgar Hoover, Congress, and the general public. So the long-term indications for the Court's protection for communists was limited.

But the First Amendment implications of *Sweezy*, though subtle at the time, were more profound and lasting jurisprudentially. *Sweezy*'s significance in First Amendment doctrine cannot be gainsaid. What started as a cogently articulated but losing idea in the Edgerton Dissent in the late 1940s had blossomed in the Douglas Concurrence in *Rumely* in 1952, and now had expanded into the thinking of the traditional judicial conservative Justice Frankfurter in *Sweezy*. The Court was developing a majority for the principle. Frankfurter did not waver. Liberals Warren and Brennan were soon to join. It surely represented an emerging majority position for the kind of constitutional protection of political association and privacy that the Hollywood Ten had hoped for. A decade later, the First Amendment doctrine of political privacy had reached its tipping point. And it would tip into consensus Supreme Court jurisprudence the following year in the famous case of *NAACP v. Alabama*, to be treated in the next chapter. ■

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

Lee E. Goodman
202.719.7378
lgoodman@wileyrein.com

Endnotes

[1] Robert M. Lichtman, *The Supreme Court and McCarthy Era Repression: One Hundred Decisions* (University of Illinois Press 2012) (collecting cases).

[2] Victor Rabinowitz, *Unrepentant Leftist: A Lawyer's Memoir* (University of Illinois Press 1996) at p. 130.

[3] 18 U.S.C. § 2385.

[4] Arthur J. Sabin, *In Calmer Times: The Supreme Court and Red Monday* (University of Pennsylvania Press 1999), at p. 11 ("Following the *Dennis* decision in 1951, fifteen groups of multiple defendants (second-string state Party leaders) were indicted and prosecuted between 1951 and 1953; the lower courts, using *Dennis* as precedent, affirmed convictions in all but one Smith Act case.") & at p. 12 ("Between 1948 and 1957, 129 indictments were obtained against alleged CPUSA members. Convictions were secured and sustained by federal appellate courts, including the Supreme Court, in almost every case until June 17, 1957.").

[5] *United States v. Dennis*, 183 F. 2d 201 (2d Cir. 1950)

[6] *Dennis v. United States*, 341 U.S. 494 (1951).

continued on page xx

continued from page x

[7] *Id.* at 581 (Black, dissenting).

[8] United States Senate, *The Censure Case of Joseph McCarthy of Wisconsin* (1954) (https://www.senate.gov/artandhistory/history/common/censure_cases/133Joseph_McCarthy.htm). For a point-by-point defense of McCarthy and his investigations *see* M. Stanton Evans, *Blacklisted by History: The Untold Story of Senator Joe McCarthy and His Fight Against America's Enemies* (Crown Publishing 2007).

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

[10] N.H. Rev. Stat. Ann. 1955, c. 588, § 1 (1955).

[11] John Bellamy Foster, "The Commitment of an Intellectual: Paul M. Sweezy (1910-2004)," Monthly Review (Oct. 1, 2004), *citing* "The Unorthodox Ideas of Radical Economists Win a Wider Hearing," *Wall Street Journal* (Feb. 11, 1972); John Kenneth Galbraith, *Economics in Perspective* (Boston: Houghton Mifflin, 1987) at p. 189.

[12] *See, e.g.,* Paul Marlor Sweezy, *The Theory of Capitalist Development* (Monthly Review Press 1942); Paul M. Sweezy, *Theory of Capitalist Development* (Dennis Dobson Ltd. 1946); Paul M. Sweezy, *Socialism* (McGraw Hill Books 1949); Paul M. Sweezy (editor), *Lenin Today: Eight Essays on the Hundredth Anniversary of Lenin's Birth* (Monthly Review Press 1971); Paul M. Sweezy, *Four Lectures on Marxism* (Monthly Review Press 1981).

[13] Available at www.MonthlyReview.org.

[14] Sweezy's full statement is reprinted at footnote 6 of *Sweezy v. New Hampshire*, 354 U.S. 234 (1957).

[15] *Id.*

[16] *Id.*

[17] *Sweezy v. New Hampshire*, 354 U.S. 234, 238 (1957).

[18] *Id.* at 241-242.

[19] *Id.* at 244.

[20] *Id.* at 243-244. Sweezy's refusal to answer questions about his lecture at the University of New Hampshire gave rise to an entirely distinct First Amendment jurisprudential principle of *academic freedom*, which is often touted by faculty on college campuses today. That subject is beyond the scope of this article on the First Amendment right of political privacy.

[21] *Id.* at 244-245.

[22] *Wyman v. Sweezy*, 100 N.H. 103, 121 A.2d 783 (1956).

[23] *Sweezy v. New Hampshire*, 352 U.S. 812 (1956)

[24] 354 U.S. 298 (1957).

[25] 354 U.S. 363 (1957).

[26] 354 U.S. 178 (1957).

[27] *Id.* at 215.

[28] *Id.* at 217 (Frankfurter, concurring).

[29] *Id.* at 185.

[30] *Id.*

[31] 354 U.S. 234 (1957).

[32] Arthur J. Sabin, *In Calmer Times: The Supreme Court and Red Monday* (University of Pennsylvania Press 1999) at p. 1.

[33] 354 U.S. at 245.

[34] *Id.* at 250.

[35] *Id.* at 254.

[36] *Id.* at 254-255.

[37] Sabin at p. 157-158.

[38] 354 U.S. at 265.

[39] *Id.* at 266-267.

[40] Sabin at p. 11.

[41] *See, e.g., Barenblatt v. United States*, 360 U.S. 109 (1959); *Uphaus v. Wyman*, 360 U.S. 72 (1959).

Events & Speeches

"The HIPAA Privacy Rule 15 Years Later: What's Next?" Workshop

Future of Privacy Forum

Kirk J. Nahra, Panelist

December 4, 2018 | Washington, DC

Mastering the Evolving Law of Data Analytics

AHIMA Data Institute: Making Information Meaningful

Kirk J. Nahra, Speaker

December 6, 2018 | Las Vegas, NV

"The Exchange" Data Privacy and Cybersecurity Forum

Today's General Counsel Institute

Matthew J. Gardner, Co-Chair

December 13, 2018 | Los Angeles, CA

Privacy in the New World Order Part II: Globalization

West LegalEdcenter

Kirk J. Nahra, Speaker

December 17, 2018

"The Path Towards a New and Complete Consumer Health Privacy and Security Regulatory Structure."

28th National HIPAA Summit

Kirk J. Nahra, Speaker

March 5, 2019 | Washington, DC

"Regulatory Challenges For Digital Health – The Emerging Law and Filling The Gaps,"

ABA Health Law Section Emerging Issues Conference

Kirk J. Nahra, Panelist

March 13-16, 2019 | Orlando, FL

Privacy Boot Camp

IAPP 2019 Global Privacy Summit

Kirk J. Nahra, Speaker

May 1, 2019 | Washington, DC

Contributing Authors

Megan L. Brown	202.719.7579	mbrown@wileyrein.com
Michael L. Diakiwski	202.719.4081	mdiakiwski@wileyrein.com
Lee E. Goodman	202.719.7378	lgoodman@wileyrein.com
Bruce L. McDonald	202.719.7014	bmcdonald@wileyrein.com
Kirk J. Nahra	202.719.7335	knahra@wileyrein.com
Duane C. Pozza	202.719.4533	dpozza@wileyrein.com
Kathleen E. Scott	202.719.7577	kscott@wileyrein.com