AN A.S. PRATT PUBLICATION
JANUARY 2019
VOL. 5 • NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 5 | NUMBER 1 | JANUARY 2019

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [5] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [1] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2019–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

White House Releases "National Cyber Strategy"

John A. Horn and Bethany L. Rupert*

The authors of this article discuss the National Cyber Strategy, which offers a comprehensive set of objectives such as the preservation of a free, open, and secure internet, while also signaling tougher repercussions for nations and criminals that engage in malicious cyber activity.

The White House released its long-awaited National Cyber Strategy[1] (the "Strategy"), offering a comprehensive set of objectives such as the preservation of a free, open, and secure internet, while also signaling tougher repercussions for nations and criminals that engage in malicious cyber activity. The Strategy is similarly ambitious in its expectations for enhanced partnerships between federal agencies and private sector entities and foreign governments. That said, this expansive list of priorities includes few specific actions or steps to implement or accomplish the stated goals, and will require concurrence from private sector businesses and foreign governments that may be reluctant to fully jump into these initiatives. In short, as with many strategic plans, it is a thorough and thoughtful approach but lacks concrete action items and will require significant diplomacy to achieve the anticipated buy-in.

THE FOUR PILLARS

The Strategy is centered around four pillars:

1) protecting against cyber threats by strengthening U.S. government and private information networks, securing critical infrastructure, and enhancing cybercrime enforcement efforts;
2) boosting the digital economy by promoting innovation in the technology sector, guarding intellectual property, and increasing the ranks of our cybersecurity workforce;
3) combating cyber threats and preserving the United States' superiority in safeguarding the internet through taking aggressive actions (thus far unidentified) if necessary; and
4) promoting an open and free internet.

* John A. Horn, a partner at King & Spalding LLP and a former Atlanta U.S. Attorney, specializes in government and internal investigations, white collar criminal defense, and crisis management. Bethany L. Rupert is an associate in the Special Matters/Government Investigations Practice Group at the firm focusing on white-collar criminal defense, internal corporate investigations and corporate compliance reviews, and civil litigation. The authors may be reached at jhorn@kslaw.com and brupert@kslaw.com, respectively.

[1] https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

The Strategy's most expansive set of objectives are protective in nature, ranging from centralizing and increasing the resiliency of federal agency IT networks, to improving space and maritime cybersecurity, protecting election and other critical infrastructure, and aiding partner nations' cyber enforcement capacity. To combat cybercrime, the Strategy emphasizes "[t]he prompt reporting of cyber incidents to the Federal Government," as well as the implementation of "standards and best practices that deter and prevent current and evolving threats and hazards in all domains of the cyber ecosystem."[2]

To bolster national defenses against attacks, the Strategy emphasizes that federal cybersecurity efforts will hinge on support from private industry. For example, the Administration expects information technology companies and tech start-ups to work with government agencies and law enforcement to "to confront challenges presented by technological barriers, such as anonymization and encryption technologies,"[3] and to use artificial intelligence and quantum computing to deter cyber threats. The Strategy identifies seven industries with which the government will prioritize building relationships and sharing information: "national security, energy and power, banking and finance, health and safety, communications, information technology, and transportation."[4] Several are singled out for special attention: for example, recognizing that "[i]nformation and communications technology (ICT) underlies every sector in America," the White House plans to work with ICT providers to improve ICT security by sharing classified threats with ICT providers who have been "cleared" for such information.

WILL THERE BE CENTRALIZED FEDERAL REGULATION?

One frequent criticism of current federal cybersecurity policy is the lack of a cohesive national regulatory structure, such that myriad agencies and state regulators have enacted a hodge-podge of security standards and breach notification rules. The Strategy recognizes the increasing number of agencies regulating in this space and pledges to clarify their roles and responsibilities, as well as their "expectations on the private sector related to cybersecurity risk management and incident response."[5] The Strategy further recognizes the importance of reporting cyber incidents to the federal government "by all victims, especially critical infrastructure partners," but offers no details regarding the manner in which this reporting will occur. It is hard to guess exactly what the Administration has in mind here; certainly, the language hints of more

[2] The White House, "National Cyber Strategy of The United States Of America," September 2018, *available at* https://www.whitehouse.gov/wp-content/uploads/2018/09/national-cyber-strategy.pdf, p. 10-11, 15.

[3] *Id.* at p. 10.

[4] *Id.* at p. 8-9.

[5] *Id.* at p. 8.

centralized federal regulation of data security and breach notification, but it is also telling that the document intentionally omits any specific recommendations or plans to achieve this goal.

A DRASTIC SHIFT

The Strategy's most notable and drastic shift from the policies of prior administrations comes in an explicit warning to nation-state and criminal actors alike that more aggressive responsive actions are in store for malicious cyber activity against the U.S. government, businesses, and citizens. The language is once again oblique, stating only that the United States will "develop swift and transparent consequences, which we will impose consistent with our obligations and commitments to deter future bad behavior." Recent public statements by Administration officials have added further details, as National Security Advisor John Bolton confirmed during a press conference[6] that the White House has intentionally "authorized offensive cyber operations . . . not because we want more offensive operations in cyberspace, but precisely to create the structures of deterrence that will demonstrate to adversaries that the cost of their engaging in operations against us is higher than they want to bear." Bolton did not elaborate on the nature of the offensive operations, but he confirmed that the Administration has rescinded Obama-era executive orders restricting the use of retaliatory hacking.

SAFEGUARDING DOMESTIC CRITICAL CYBER INFRASTRUCTURE

Following such widely publicized attacks to public infrastructure such as the Russian hack of the Ukranian power grid, the Strategy recognizes the need to safeguard domestic critical cyber infrastructure. To accomplish this, the White House plans to partner with private industry to "collectively use a risk-management approach to mitigating vulnerabilities to raise the base level of cybersecurity across critical infrastructure."[7] At the same time, the Administration will "develop a comprehensive understanding of national risk by identifying national critical functions and will mature our cybersecurity offerings and engagements to better manage those national risks."[8] Key to this plan is to share the information learned with the industries identified in the Strategy: "national security, energy and power, banking and finance, health and safety, communications, information technology, and transportation."[9]

---

[6] https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/09/21/the-cybersecurity-202-trump-administration-seeks-to-project-tougher-stance-in-cyberspace-with-new-strategy/5ba3e85d1b326b7c8a8d158a/?utm_term=.048b68ae030f.

[7] National Cyber Strategy, *supra* note 2, p. 8.

[8] *Id.*

[9] *Id.* at p. 8-9.

NEW TECHNOLOGIES

The continued development of new technologies also will be an important contributor to both strengthening our cyber defenses and preserving the United States' role as an influencer in global cyber policymaking. Specifically, "[t]he Administration will work across stakeholder groups, including the private sector and civil society, to promote best practices and develop strategies to overcome market barriers to the adoption of secure technologies."[10]

Additionally, to promote an open internet, the Administration plans to support and encourage "open, industry-led standards activities based on sound technological principles."[11] The objective of the White House in promoting such developments and standards is to "advance American influence" and ultimately protect the nation from further threats.

CONCLUSION

In sum, much remains to be seen in terms of proposing specific steps to accomplish the many objectives and achieve the broad platitudes in this document. One of the biggest questions moving forward will be the receptiveness of the private sector and foreign governments to the invitations to partner with the White House to solve these challenges. Would-be partners in Silicon Valley and elsewhere have expressed reservations about the government's policies on encryption, and companies often have mixed views about fulsome sharing with the government about cyber threats and incidents. Corporations have a duty to abide by not only the privacy and security laws of the United States, but also those of other countries in which they operate. And as foreign jurisdictions are enacting increasingly strict limitations regarding the transfer of data outside their borders, many of these countries are expressing increasing reservations about U.S. data privacy laws and procedures.

Still, those attitudes may change in the coming months and years as Congress ramps up to consider its own federal legislation on data privacy. In a Senate hearing on September 26, 2018 involving some of the nation's largest tech and communications companies, several senators expressed readiness to pass a law similar in effect to the EU's General Data Protection Regulation ("GDPR") or the California Consumer Privacy Act. Sen. Brian Schatz (D-Hawaii)[12] said that, although he understood the concerns of tech and communications companies, such companies should not expect Congress to "replace a progressive California law – however flawed you may think it is – with a nonprogressive federal law." In a second hearing on this topic held on

[10] *Id.* at p. 14.

[11] *Id.* at 25.

[12] https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/09/27/the-cybersecurity-202-senate-hearing-highlights-challenges-of-crafting-national-privacy-law/5babbb8a1b326b7c8a8d16aa/?utm_term=.ff5c40b3368b.

October 10, 2018, senators listened to the viewpoints of privacy advocates, who reinforced the need for a federal law, and stressed that this law should work alongside state laws, rather than preempting them, and that the law should be backed with enforcement authority from the Federal Trade Commission or a new federal agency. Although some legislators have expressed concerns about fashioning the law in this manner, or creating something similar to the California law or the GDPR, there appears to be some agreement that federal privacy legislation is necessary to bring coordination to 50 different state laws that vary significantly. As stated by Committee Chairman Senator John Thune (R-SD),[13] "The question is no longer whether we need a law for consumer data privacy, the question is what shape these laws will take."

[13] https://mashable.com/article/tech-industry-consumer-data-protection-senate-hearing/#iuyFcW9y-JiqR.