AN A.S. PRATT PUBLICATION
JULY/AUGUST 2018
VOL. 4 • NO. 6

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 4 NUMBER 6 JULY/AUGUST 2018

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*, [4] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [167] (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

(2018–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.

Enhancing Cyber Threat Information Sharing

By Steven G. Stransky*

The narrow set of recovery options for the private sector on the back end of a cyberattack reinforces the need to have robust security systems in place on the front end. The author of this article discusses why the executive branch must streamline and consolidate its disparate offices and programs responsible for sharing cyber threat information so that the private sector can succeed in adequately protecting its networks from intrusion on the front end.

The scale and sophistication of cyberattacks against the private sector in the United States continue to expand at an alarming rate. However, there are limited mechanisms available for a cyberattack victim to recover damages, and a decision by the U.S. Court of Appeals for the D.C. Circuit has further limited avenues for relief in circumstances in which the hacker is a hostile foreign government. The narrow set of recovery options for the private sector on the back end of a cyberattack reinforces the need to have robust security systems in place on the front end. In order for the private sector to succeed in adequately protecting its networks from intrusion on the front end, however, the executive branch must streamline and consolidate its disparate offices and programs responsible for sharing cyber threat information.[1]

(FINALLY) A CONSENSUS IN WASHINGTON: FOREIGN GOVERNMENTS AND THREATS TO CYBERSECURITY

Although the differences between the political parties in Washington, D.C. seem to be emphasized more than their similarities, there is at least one issue on which both sides readily agree: cyberattacks by foreign governments and other foreign adversaries represent a significant threat to both the public and private sectors. In fact, both the Obama and Trump administrations have provided very similar intelligence assessments as to the nature, scope, and significance of recent cyberattacks effectuated by foreign governments.

For example, James R. Clapper, who served as the Director of National Intelligence ("DNI") in the Obama administration, identified Russia, China, Iran, and North Korea,

* Steven G. Stransky is senior counsel in the Business Litigation and Privacy & Cybersecurity practice groups of Thompson Hine LLP. Prior to joining the firm, Mr. Stransky served in the federal government, including as Deputy Legal Adviser to the President's National Security Council and as Senior Counsel at the U.S. Department of Homeland Security's Intelligence Law Division. He may be contacted at steve.stransky@thompsonhine.com.

[1] The federal government defines "cyber threat information" as "any information that can help an organization identify, assess, monitor, and respond to cyber threats." The U.S. Department of Commerce, National Institute of Standards and Technology, Special Pub. 800-150: Guide to Cyber Threat Information Sharing, at iii (Oct. 2016).

among others, as "[l]eading [t]hreat [a]ctors" in the cyber field.[2] More specifically, in a 2016 briefing to Congress, Clapper stated that "Russia is assuming a more assertive cyber posture" and that "North Korea probably remains capable and willing to launch disruptive or destructive cyberattacks to support its political objectives."[3] He also noted that "China continues to have success in cyber espionage against the US Government, our allies, and US companies."[4] Daniel R. Coats, who succeeded Clapper as the DNI in the Trump administration, reached similar conclusions regarding state-sponsored cyberattacks. For instance, in a 2017 briefing to Congress, Coats also identified Russia, China, Iran, and North Korea, among others, as "[c]yber [t]hreat [a]ctors."[5] Coats described Russia as "a full-scope cyber actor that will remain a major threat to US Government, military, diplomatic, commercial, and critical infrastructure" and stated that "Moscow has a highly advanced offensive cyber program, and in recent years, the Kremlin has assumed a more aggressive cyber posture."[6] "Tehran," according to Coats, "continues to leverage cyber espionage, propaganda, and attacks to support its security priorities, influence events and foreign perceptions, and counter threats. . . . "[7] Last, regarding North Korea, Coats found that "Pyongyang has previously conducted cyberattacks against US commercial entities – specifically, Sony Pictures Entertainment in 2014" and noted that the regime "remains capable of launching disruptive or destructive cyberattacks to support its political objectives."[8]

This dire assessment of cyber threats is not isolated to the executive branch. One only has to look to the multiple hearings, draft legislation, and statements originating from Congress to see that both parties on the Hill recognize the significance of this issue. For example, John Ratcliffe (a Texas Republican) has overseen congressional hearings that examined the "evolving cybersecurity threats from nation-states such as China, Russia, North Korea and Iran."[9] According to Ratcliffe, "[t]o put it simply, cybersecurity is national security."[10] Similarly, Jim Langevin (a Rhode Island Democratic) has framed the debate around cybersecurity as "an issue that is of critical

[2] James R. Clapper, "Worldwide Threat Assessment of the US Intelligence Community," Statement for the Record for the Senate Armed Services Committee, at 3 (February 9, 2016).

[3] *Id.*

[4] *Id.*

[5] Daniel R. Coats, "Worldwide Threat Assessment of the US Intelligence Community," Statement for the Record for the Senate Armed Services Committee, at 1-2 (May 11, 2017).

[6] *Id.* at 1.

[7] *Id.*

[8] *Id.* at 2.

[9] Statement of John Ratcliffe, Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee, House Homeland Security Committee, "Emerging Cyber Threats to the United States," at 1 (February 25, 2016).

[10] *Id.*

importance not only to our national security, but also to our economic security, affecting every American consumer and investor."[11]

There is broad consensus that foreign governments, among other adversaries, continue to utilize novel tactics, techniques, and procedures to threaten and harm a broad range of private sector businesses inside the United States. Congress, through legislation, and presidents, through executive directives, have sought to mitigate the risks posed by these types of cyber threats. However, as will be explained next, private sector entities continue to have limited recourse to recover losses in situations where foreign governments are responsible for the cyberattack.

CYBERSECURITY, CIVIL REMEDIES, AND SOVEREIGN IMMUNITY

Much of the media coverage on recent cyberattacks (e.g., Uber, Equifax, Target) focuses on whether individuals who have had their personal information compromised through a data breach can recover damages from the business that was hacked. Given the anonymity of the hacker, there is less of a focus on whether the business that was subject to the cyberattack itself can recover damages from the person or groups that initiated the cyberattack. In other words, in the event of a data breach, the consumer blames the business that retained their personal information, and the business blames the anonymous hackers. . .who cannot be reached for comment.

This pattern underscores the difficulty in using civil proceedings to redress the harm caused by a hacker. The first hurdle, which is often the most challenging, is identifying the perpetrator of the cyberattack. It is often difficult, at least from a technical perspective, to identify the person or entity that is responsible for undertaking the types of sophisticated cyberattacks that have recently occurred in the United States and across the globe. As one commentator noted, "[a]ttribution [of a cyberattack] can occur, but usually does so via secondary intelligence, dumb mistakes, or some admission of responsibility in lieu of tracing attacks back to their original source."[12]

Next, assuming that the identity of the hacker can be discovered, the Foreign Sovereign Immunity Act of 1976 ("FSIA")[13] provides another obstacle to the recovery of damages wherein a foreign government is identified as the perpetrator of the cyberattack. The FSIA provides the sole basis for obtaining jurisdiction over a foreign state in U.S. federal court and the law broadly dictates that unless an exception in FSIA is applicable to a specific case, "a foreign state shall be immune from the jurisdiction of the courts of the United States."[14] In *Doe v. The Federal Democratic*

[11] Congressional Record Volume 160, Number 109 (July 14, 2014).

[12] Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 Harv. Int'l L.J. 374, 399 (2011).

[13] Pub. L. 94-583, 90 Stat. 289l (1976) (codified as amended at 28 U.S.C. §§ 1330, 1391(f), 1441(d), and 1602-11).

[14] 28 U.S.C.§ 1604.

Republic of Ethiopia,[15] the D.C. Circuit analyzed one of FSIA's exceptions to sovereign immunity – the noncommercial-tort exception – in the context of a foreign government's liability for undertaking a cyberattack in the United States. This particular exception abrogates sovereign immunity in cases involving personal injury, death, or property damage or loss occurring in the United States and caused by the tortious act of, *inter alia,* a foreign state.[16]

In *Doe*, the plaintiff (a U.S. citizen born in Ethiopia) was an active member of the Ethiopian diaspora who worked to publicize corruption and human rights issues in Ethiopia. He alleged that he was "tricked" into downloading spyware onto his personal computer in Maryland that "allegedly enabled [Ethiopia] to spy on him from abroad."[17] In short, the D.C. Circuit found that the noncommercial-tort exception only "abrogates sovereign immunity for a tort occurring *entirely* in the United States."[18] The court reasoned that because Ethiopia's "intent to spy" on the plaintiff and its "initial dispatch" of the spyware toward the plaintiff's computer "occurred outside the United States," then the underlying tort could not have occurred "entire[ly] in the United States."[19] Consequently, the court found that the noncommercial-tort exception was inapplicable to the plaintiff's case.

The D.C. Circuit's decision in *Doe* reinforces the difficulties in using civil proceedings to obtain damages as a result of a cyberattack. As such, much of the focus in the cybersecurity realm has been on strengthening existing computer networks in order to deter and avoid unlawful intrusion. The federal government has timely and actionable intelligence on cyberattack tactics, techniques, and procedures; however, it needs to streamline and consolidate its information sharing processes and programs to better enable the private sector to protect its own networks.

ENHANCING CYBER THREAT INFORMATION SHARING

In recent years, the federal government has undertaken several different initiatives to strengthen cybersecurity information sharing within and among the public and private sectors. For example, during his tenure in office, President Obama issued multiple executive orders related to cybersecurity, including "Improving Critical Infrastructure

[15] 851 F.3d 7 (D.C. Cir. 2017).

[16] 28 U.S.C.§ 1605(a)(5). The noncommercial-tort exception to sovereign immunity itself contains exemptions to its general rule. *Id.* at § 1605(a)(5)(A)-(B).

[17] *Doe*, 851 F.3d at 8.

[18] *Id.* (emphasis in original).

[19] *Id.* at 11.

Cybersecurity"[20] and "Promoting Private Sector Cybersecurity Information Sharing."[21] The former sought to, *inter alia*, increase the dissemination of cyber threat information from the federal government to the private sector; expedite the processing of security clearances to private sector entities; and initiate the development of a cybersecurity framework. The latter, as evident by its title, encouraged the sharing of cybersecurity threat information within the private sector and between the private sector and the federal government, and urged for the development of information sharing and analysis organizations to serve as focal points for cybersecurity information sharing and collaboration. Through the Cybersecurity Information Sharing Act of 2015,[22] Congress provided additional legal authority for cybersecurity information sharing between and among the private sector; state, local, tribal, and territorial governments; and the federal government. The law also grants liability protection to companies that share, in accordance with federal guidelines and rules, certain types of cyber threat information with the federal government.

The federal government has recognized that it is better situated than the private sector to detect and analyze cyber threats emanating from foreign adversaries, including hostile foreign governments, and there is a profound need for the government to share this information with a broad range of nongovernmental actors. Unfortunately, the federal government has implemented its cyber threat information sharing programs in a fragmented and inchoate manner. More specifically, the federal government has dozens of information sharing programs that are scattered among multiple departments and agencies, with some departments having a multitude of overlapping programs. For example, the Department of Homeland Security ("DHS") alone has several offices and programs dedicated to engaging with the private sector on cybersecurity issues, such as its Enhanced Cybersecurity Services Program; Cyber Information Sharing and Collaboration Program; Homeland Security Information Sharing Network; National Cybersecurity and Communications Center; Automated Indicator Sharing Initiative; and Critical Infrastructure Partnership Advisory Council. Not only are these offices within DHS competing internally for audiences (and, of course, congressional funding), they are also competing with information sharing programs operated from within other departments and agencies, including the Defense Department's Cybersecurity Program and Cyber Crime Center; the Department of Energy's Cyber Risk Information Sharing Program; and

[20] Exec. Order 13636, 78 Fed. Reg. 33, 11739 (Feb. 12, 2013).

[21] Exec. Order 13691, 80 Fed. Reg. 34, 9349 (Feb. 13, 2015). President Trump recently issued his own executive order on cybersecurity, titled "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." Exec. Order 13800, 82 Fed. Reg. 92, 22391 (May 11, 2017). Although the order primarily focused on safeguarding the federal government's information technology networks, it also mandated that the executive branch use its legal authorities and capabilities to support risk management efforts related to critical infrastructure.

[22] Pub. L. 114-113, 129 Stat. 694 (2015) (codified as amended at 6 U.S.C. § 1501-1510).

the Federal Bureau of Investigation's National Cyber Investigative Joint Task Force, InfraGard Program, and Domestic Security Alliance Council.

Each information sharing program and office has its own set of procedures and guidelines dictating which private sector businesses can become members of or otherwise participate in the program. These governing rules, much like the acronyms used to identify the programs (e.g., CRISP, CISCP, NCCIC, and NCIJTF), can be confusing and hard to comprehend. It is often difficult for members of the private sector, especially those that have cross-sector responsibilities, to identify from which federal agency they should be seeking information on threats to cybersecurity. Moreover, if a private sector company is fortunate to be a member of one of these information sharing programs, there will undoubtedly be ambiguity as to whether the information it is receiving represents the total spectrum of cyber threats facing its business or whether other federal agencies are presenting other relevant cyber threat information through their separate programs.

In order for the private sector to be successful in protecting its own networks from cyberattacks, the executive branch must streamline and consolidate its disparate cyber threat information sharing programs. One potential solution to this problem is for the federal government to create a single office – a Cyber Threat Ombudsman Office – that interfaces with the private sector on all cyber threat information issues. In this context, it would be the responsibility of the Ombudsman to scour the different cyber threat information programs within the federal government in order to provide the private sector requestor with one consolidated report on the threats and vulnerabilities facing the business (individually) or the sector (more generally). Given the nature and sensitivity of information pertaining to cyber threats, these reports could further be delineated based on security clearance classification or similar access restrictions. Having such a "one-stop" source of cyber threat information would allow private sector entities to more efficiently gain access to the cyber threat information they need to understand and minimize the vulnerabilities in their own businesses.

Given that the proposal for a Cyber Threat Ombudsman Office could potentially need congressional authorization and appropriations, it may be difficult to accomplish in the near term. However, a similar approach could be taken at the department- or agency-level without the need for legislative approval. For instance, having a DHS Cyber Ombudsman that would be the interface between the private sector and the Department could have similar benefits as the proposal described above and could be accomplished with simple internal reorganization. More specifically, it would be the responsibility of the DHS Cyber Ombudsman to coordinate behind the scenes in the department – between its intelligence, law enforcement, and cybersecurity experts – in order to provide the private sector requestor with one consolidated cyber threat report or assessment. Again, given the multiple cybersecurity-related offices and programs within the Departments of Homeland Security, Defense, and Justice, such an

Ombudsman within each department would streamline both the access and responses to cyber threat information.

If the federal government refrains from taking any action to consolidate its information sharing offices and programs, there are measures that the private sector can undertake to improve its access to the federal government's cyber threat information. For instance, depending on its size and structure, a private sector business could consider hiring an employee or contractor whose sole responsibility is to ensure that it is included in all of the federal government's information sharing programs. The responsibility of this official may include establishing accounts for online information sharing portals, accessing cyber threat bulletins and alerts, ensuring registration for cybersecurity training courses, and requesting or participating in (classified and unclassified) threat briefings provided by the federal government. Private sector companies may be able to leverage the expertise and personnel within an existing Chief Information Office or Government Relations Office to satisfy this requirement.

Whatever the approach may be, it is clear that until the federal government alters its structure and approach to sharing cyber threat information, the private sector will continue to spend unnecessary time, resources, and personnel navigating the labyrinth of federal information sharing programs and offices.