AN A.S. PRATT PUBLICATION
NOVEMBER/DECEMBER 2015
VOL. 1 • NO. 3

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 1 NUMBER 3 NOVEMBER/DECEMBER 2015

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) 487-3000
Fax Number .... (518) 487-3584
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 ..... (518) 487-3000

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*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [82] (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

(2015–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, 718.224.2258. 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.

Cybersecurity and Government "Help" – Engaging with DOJ, DHS, FBI, Secret Service, and Regulators – Part II

By Alan Charles Raul and Tasha D. Manoranjan*

In this two-part article, the authors provide an overview of government cybersecurity resources, and encourage companies to consider whether and when it makes sense to take advantage of this assistance. The first part, which appeared in the October 2015 issue of Pratt's Privacy & Cybersecurity Law Report*, introduced the jurisdictional landscape and cybersecurity resources available from the Department of Justice and the Department of Homeland Security. This second part of the article discusses the cybersecurity resources available from the Federal Bureau of Investigation, the United States Secret Service, and regulators.*

FEDERAL BUREAU OF INVESTIGATION

The Federal Bureau of Investigation offers many opportunities for collaboration with the private sector, through partnerships such as the National Cyber Forensics and Training Alliance ("NCFTA"), InfraGard, and the Cyber Action Team. NCFTA was created in 1997 to bring together law enforcement, private industry and academia to share information to stop emerging cyber threats and mitigate existing ones.[1] NCFTA operates as an early warning system, to enable the quick dissemination of information about new threats facing companies. NCFTA members then create strategies to help mitigate the threat posed, and FBI agents use this information to further FBI investigations.

InfraGard is a partnership between the FBI and the private sector, including businesses, academic institutions, and others working to share information and prevent cyber crime. Members of InfraGard have access to the FBI's iGuardian reporting platform, enabling partners within critical infrastructure sectors to distribute alerts and bulletins about network intrusions. Members are encouraged to report specifics to the FBI, which are then provided to CyWatch, the FBI's 24/7 cyber operations

---

* Alan Charles Raul, a member of the Board of Editors of *Pratt's Privacy & Cybersecurity Law Report*, is a partner at Sidley Austin LLP, where he is the leader of the Privacy, Data Security and Information Law practice. Tasha D. Manoranjan is an associate in the firm's Privacy, Data Security and Information Law practice. Resident in the firm's Washington, D.C., office, the authors may be reached at araul@sidley.com and tmanoranjan@sidley.com, respectively.

[1] Federal Bureau of Investigation, The NCFTA: Combining Forces to Fight Cyber Crime, Sept. 16, 2011, *available at* https://www.fbi.gov/news/stories/2011/september/cyber_091611 (last accessed July 6, 2015).

center in which agents and analysts triage the issue, notify previously unknown victims, and assign leads to field offices for further investigation.[2]

The Cyber Action Team ("CAT") is a rapid deployment group of cyber experts who can provide investigative support and mitigate risks. CAT is deployed by the FBI on major computer intrusions and cyber-related emergencies.[3] CAT is composed of special agents and computer scientists who are highly trained in computer languages, forensic investigations and malware analysis. Companies can reach out to their local FBI field office to contact the nearest Cyber Task Force, which can then bring in CAT as appropriate.

The FBI has seen an 80 percent increase in the number of computer intrusion investigations since 2002, and has thus "developed a number of innovative staffing programs and collaborative private industry partnerships to ensure that over the long term we remain focused on our most vital resource – our people."[4] One example showcasing the FBI's success drawing on its public-private relationships, as well as its work with international law enforcement, is the capture and prosecution of Aleksandry Andreevich Panin, who pled guilty to conspiracy to commit wire and bank fraud in January 2014 for developing and distributing malicious software known as Spyeye.[5] Spyeye infected more than 1.4 million computers in the United States and internationally, according to the FBI. Members of the financial services industry reported more than 10,000 bank accounts were compromised by Spyeye, and shared information with the FBI to counter this cyber threat.[6] Panin's co-conspirator, Hamza Bendelladj, was arrested in January 2013 in Bangkok.

Another example of the FBI's collaboration with the financial sector is its efforts to disrupt the GameOver Zeus botnet, believed to be responsible for stealing millions of dollars from American and foreign businesses and consumers.[7] GameOver Zeus is malware designed to steal banking and other credentials from computers, and then redirect wire transfers to criminals' accounts. It is estimated to have stolen over $100 million. The FBI's efforts to disrupt GameOver Zeus "involved notable cooperation with the private sector and international law enforcement."[8]

---

[2] Federal Bureau of Investigation, iGuardian: The FBI's Industry-Focused Cyber Intrusion Reporting Platform, *available at* https://www.fbi.gov/stats-services/iguardian (last accessed July 6, 2015).

[3] Federal Bureau of Investigation, The Cyber Action Team: Rapidly Responding to Major Computer Intrusions, Mar. 4, 2015, *available at* https://www.fbi.gov/news/stories/2015/march/the-cyber-action-team (last accessed July 6, 2015).

[4] Robert Anderson, Jr., Executive Assistant Director, Criminal, Cyber, Response, and Services Branch of Federal Bureau of Investigation, Statement Before the Senate Committee on Homeland Security and Governmental Affairs (September 10, 2014) (Washington, D.C.), https://www.fbi.gov/news/testimony/cyber-security-terrorism-and-beyond-addressing-evolving-threats-to-the-homeland.

[5] *Id.*

[6] *Id.*

[7] *Id.*

[8] *Id.*

UNITES STATES SECRET SERVICE

The Secret Service may be best known for its responsibility for protecting the President. However, the Secret Service is one of the federal authorities at the forefront of investigating and resolving transnational cyber criminal threats that threaten U.S. businesses. Since 1984, the Secret Service has been tasked with investigating the federal crimes of unauthorized access to computers and access device fraud.[9] The Secret Service is eager to cultivate strong public-private partnerships to successfully fight computer intrusions and reduce cyber risk, to the welcome benefit of companies. In 2013, the Secret Service's efforts resulted in the prevention of over $1.1 billion of losses due to cyber crime.[10]

The Secret Service proactively investigates and attempts to identify and infiltrate transnational cyber criminal groups. The Secret Service has a global network of field offices, including 39 Electronic Crimes Task Forces ("ECTFs") which maintain relationships between businesses, federal, state and local law enforcement officials to prevent, detect and investigate cyber crimes.[11] The Secret Service encourages companies to proactively join and engage with their local ECTF, which can facilitate information sharing and access to other cybersecurity resources. The Secret Service has found, "These [Electronic Crimes] task forces have resulted in the identification, development, and implementation of tools and methodologies that entirely eliminate what were previously actively exploited technological vulnerabilities."[12] Given the speed with which technological threats adapt and proliferate, effective information sharing with public and private sector partners can assist all partners in strengthening cybersecurity defenses.

When the Secret Service identifies what appears to be a potential network intrusion, the Secret Service contacts the owner of the computer system to assess the data breach and stop the continued theft of information. During this investigation, the Secret Service attempts to identify malware and the means of access used in the intrusion. This information is then shared with the cybersecurity community to enable other companies to mitigate their own cyber risk. Given companies' reputational risks, the Secret Service strives to protect the privacy and confidentiality of the victim company;

---

[9] 18 U.S.C. §§ 1029 – 1030.

[10] Department of Homeland Security, U.S. Secret Service Annual 2013 Report (2013), *available at* http://www.secretservice.gov/USSS_FY13AR.pdf.

[11] *Electronic Crimes Task Forces and Working Groups*, U.S. Secret Service, http://www.secretservice.gov/ectf.shtml (last visited July 10, 2015).

[12] Matthew Noyes & Ari Baranoff (United States Secret Service), *Corporate-Government Engagement/Public-Private Partnerships*, *in Cybersecurity: A Practical Guide to the Law of Cyber Risk* 4-1, 4-4 (Ed McNicholas & Vivek Mohan eds., forthcoming 2015).

indeed, the Secret Service recognizes that, "[f]undamental to these trusted [public-private] relationships is a commitment to protecting victims' privacy and the confidentiality of their information."[13]

The Secret Service worked with Target Corporation to mitigate the effects of the data breach Target suffered in 2013. The Secret Service and DOJ notified Target on December 12, 2013, that Target may have suffered a payment card data breach.[14] The next day, the Secret Service started working with Target and independent investigators hired by Target to identify the criminals' means of entry. Target confirmed they had experienced a data breach and began blocking the criminal's access to its network on December 15. The Secret Service notes, "[p]roactive engagement with law enforcement helps to develop the policies, processes, and trusted relationships that enable such effective responses."[15]

Another example of the Secret Service's corporate assistance activity stems from an advisory published July 31, 2014 by the Secret Service, NCCIC and the Financial Services – Information Sharing and Analysis Center ("FS-ISAC"). The advisory identified malware dubbed "BACKOFF" that was being used to obtain payment card data from point-of-sale systems.[16] Within approximately three weeks, UPS Store, Inc. confirmed that they identified 51 stores in 24 states that had been affected by BACKOFF, and were then able to remove this malware from their systems. UPS was thus able to contain this data breach to one percent of its store locations. The Secret Service points out, "[t]his sort of information sharing effort likely contributed to the prevention of substantial financial losses to UPS Store Inc., their customers, and financial institutions."[17]

REGULATORS

The Security and Exchange Commission's Division of Investment Management issued guidance in April 2015 to assist investment companies and advisers in handling cybersecurity risks.[18] The SEC recommends conducting periodic assessments of internal and external cybersecurity threats, as well as established security controls. The SEC recommends having written policies, procedures and training to prevent, detect and respond to cyber threats. The SEC guidance notes that participating in the Financial Services – Information Sharing and Analysis Center ("FS-ISAC") enables funds and advisers to share cyber threat information and responses. FS-ISAC is a global

[13] *Id.* at 4-3.
[14] *Id.* at 4-10.
[15] *Id.*
[16] *Id.* at 4-11.
[17] *Id.*
[18] Securities and Exchange Commission, Division of Investment Management, Guidance Update No. 2015-02, April 2015, *available at* http://www.sec.gov/investment/im-guidance-2015-02.pdf.

resource for cyber and physical threat analysis and information sharing. FS-ISAC also assists companies by offering recommended solutions from leading industry experts.[19]

The Financial Industry Regulatory Authority ("FINRA") also released a report on cybersecurity in February 2015.[20] The report identifies principles and practices for financial firms to consider, and makes recommendations for addressing cybersecurity risks. The report recommends firms conduct risk assessments to identify and manage cybersecurity threats, as well as prepare incident response plans. FINRA's report states, "FINRA expects firms to consider the principles and effective practices presented in this report as they develop or enhance their cybersecurity programs."[21] FINRA also encourages firms to take advantage of intelligence-sharing opportunities, as a form of "collaborative self defense" for broker-dealers.[22]

The Office of the Comptroller of the Currency ("OCC") conducts ongoing monitoring and information sharing of cybersecurity issues across the financial sector. The OCC focuses on cyber threats, vulnerabilities and risk management options.[23] For example, the OCC "conveys risk management practices to banks, including strategies to identify, prevent, mitigate and respond to attacks."[24] During and after a cyber attack, the OCC helps evaluate the attack's impact to determine if the attack poses a material risk to bank systems and bank customer information. The OCC simultaneously evaluates "whether the institutions involved are taking appropriate and timely corrective action."[25] OCC examiners also conduct regular onsite examinations as part of their ongoing supervision of banks. Examiners "assess the adequacy of the controls that protect customer information, and bank systems and information."[26]

The Comptroller currently chairs the Federal Financial Institutions Examination Council ("FFIEC"), an interagency body comprised of the FFIEC's State Liaison Committee and the five federal banking regulatory agencies: the OCC, the Federal Reserve Bureau, the Federal Deposit Insurance Corporation, the National Credit Union Administration and the Consumer Financial Protection Bureau. In 2013, the FFIEC created a Cybersecurity and Critical Infrastructure Working Group

---

[19] Financial Services, Information Sharing and Analysis Center, About FS-ISAC, *available at* https://www.fsisac.com/about (last accessed July 6, 2015).

[20] Financial Industry Regulatory Authority, Report on Cybersecurity Practices, February 2015, *available at* https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf (last accessed July 6, 2015).

[21] *Id.* at 2.

[22] *Id.*

[23] Testimony of Valerie Abend, Senior Critical Infrastructure Officer, Office of the Comptroller of the Currency, before the Sen. Comm. on Banking, Housing and Urban Affairs (December 10, 2014), http://www.occ.gov/news-issuances/congressional-testimony/2014/pub-test-2014-165-written.pdf.

[24] *Id.* at 4.

[25] *Id.*

[26] *Id.* at 7.

("CCIWG") to "build on existing efforts to strengthen the activities of other interagency and private sector groups with respect to cybersecurity."[27] The CCIWG acts as a liaison between FFIEC members and government entities (intelligence, law enforcement, and DHS) regarding cybersecurity and critical infrastructure. CCIWG helps FFIEC members collaborate on cyber-related examination policy, training, cybersecurity incident responses, and information-sharing efforts.[28] Through its coordination and information sharing efforts across the public and private sectors, CCIWG has issued statements advising institutions about threats posed by ATM cashout schemes, distributed denial of service attacks, and widespread vulnerabilities such as Heartbleed and Shellshock.[29]

CONCLUSION

Companies should remember that the obligation for their own cyber security begins and ends with themselves. The government may assist companies in protecting their networks, but the government's position is that network owners are best positioned to monitor and defend their data. As Michael Daniel, President Obama's Special Assistant and Cybersecurity Coordinator, has stated, "the government should help you – private sector companies – help yourself . . . [T]he entire burden of network defense, regardless of where the threat originates, cannot fall solely on the government."[30] Indeed, a sprawling legal and regulatory scheme surrounding data protections and cybersecurity ensures companies remain cognizant of their obligations on these issues.

However, information-sharing, cooperation and partnership across public and private entities can help reduce the risks of cyber crime and ameliorate the effects after cyber crime. Building such relationships in advance of incidents can facilitate speedy detection, prevention and mitigation of cyber crime. Opportunities for such partnerships exist with nearly every interested federal authority, and companies are encouraged to consider taking advantage of these partnerships to better protect themselves from cyber threats and to cultivate a friendly enforcement climate. Companies should weigh the potential benefits against the risks inherent in inviting government attention and involvement.

---

[27] *Id.* at 9.

[28] *Id.*

[29] *Id.*

[30] Remarks of Special Assistant to the President and White House Cybersecurity Coordinator Michael Daniel, "007 or DDoS: What is a Real World Cyber?" at 3 (February 28, 2013) (RSA Conference USA 2013, San Francisco, CA), *available at* https://www.whitehouse.gov/sites/default/files/docs/2013-02-28_final_rsa_speech.pdf.