August 2, 2016

White Collar Roundup - August 2016

What Happens When a Data-Storage Provider Holds Your Data Overseas?

The U.S. Court of Appeals for the Second Circuit ruled in *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation* that the government cannot use a search warrant to obtain information about a third-party account holder whose data the company maintains overseas. The real and immediate effect for criminal-law practitioners and their clients is that there is now a new suppression argument, at least as to e-mails that the government has already obtained overseas by the now-proscribed means. The issue arose when law enforcement obtained a search warrant for certain e-mails housed on Microsoft's web-based e-mail system. It appears that Microsoft's systems store e-mails in the United States or abroad depending on an automatic analysis of the likely location of the e-mail account holder. For whatever reason, the e-mails for the account subject to the search warrant were stored in Microsoft's data center in Dublin, Ireland. In response to the warrant, Microsoft provided all responsive information held in the United States, but moved to quash the subpoena vis-à-vis the information held in Dublin. The magistrate judge denied the motion, which Microsoft appealed to the district court. The district judge also denied the motion, and ordered Microsoft to be held in civil contempt for failure to comply with the warrant. Microsoft appealed, and the Second Circuit reversed. It held that the Stored Communications Act (SCA) did not authorize the government to obtain data of a third-party account holder stored overseas by serving a warrant on a company in the United States. Notably, the court did not make any determination about the Fourth Amendment implications of the issue; its reasoning and holding applied only to the extraterritoriality of warrants issued pursuant to the SCA. The Second Circuit also did not extend this logic to the company's *own* data were the company to be served with a grand-jury subpoena.

FBI and Secret Service Want More Data Breach Notifications

The Federal Bureau of Investigation (FBI) and U.S. Secret Service (USSS) jointly filed comments on proposed Federal Communications Commission (FCC) rules "concerning the privacy of broadband customers to assist the [FCC] in evaluating law enforcement, public safety, and national security issues." The FBI and USSS agree "that the FCC should extend data breach notification requirements to broadband providers subject to the [FCC's] jurisdiction, so that voice, broadband, cable, and satellite customers will all be on equal footing if a customer's personal data is improperly obtained through the breach of a provider." Both agencies believe prompt notification to the victims and law enforcement will "minimize any damage, help identify and apprehend the perpetrators, and prevent others from being victimized." Specifically, the FBI and USSS want customers to "receive notice if their customer proprietary information has been or is reasonably believed by the Service Provider to have been accessed or acquired by an unauthorized party, unless there is no reasonable risk of harm to the customer from the compromise of the information." They also want the ability to delay notification to customers if necessary to avoid interference with a criminal investigation, and to require service providers to retain information to assist law enforcement.

Cybersecurity Protection for Interbank Transfers

Billions have been stolen through cyber attacks on financial institutions in recent months. An interim staff report from a House committee noted failures in the response by the Federal Deposit Insurance Corporation to these breaches. In the meantime, the Federal Financial Institutions Examination Council (FFIEC), representing numerous high-level government agencies, issued a statement, highlighting the need for financial institutions to "actively manage the risks associated with interbank messaging and wholesale payment networks." The statement "is intended to alert financial institutions to specific risk

mitigation techniques related to cyber attacks exploiting vulnerabilities and unauthorized entry" through client terminals. Among other suggestions, the statement admonished financial institutions to "use multiple layers of security controls to establish several lines of defense," including to address risks from compromised credentials.

Stopping TriggerFish, Stingrays and Hailstorms

We're not talking about aquatic life or extreme weather. Devices with these names are used by law enforcement to locate cell phones by mimicking a service provider's cell site to "ping" a cell phone, which then pings the device back. When it does, the agents are able to home in on the signal and find the phone, and more often than not, the subject of their investigation. In *United States v. Lambis*, Judge William H. Pauley III of the U.S. District Court for the Southern District of New York suppressed seizure as a result of the use of a TriggerFish. In that case, the Drug Enforcement Administration (DEA) was conducting a drug-trafficking investigation and had obtained a warrant to procure pen-register (record of numbers dialed) and cell-site (record of cell towers pinged) information from a target cell phone. Cell-site information might narrow down a geographic area in which the phone is being used, but it's not too specific. For example, cell phones from a five-square-block area might all ping the same tower. In New York City, that's a lot of phones. In *Lambis*, the DEA agents used a TriggerFish to force the subject cell phone to ping it. As they used it, they were directed to an apartment building. Then, agents walked the halls of the building with the device until they found the apartment with the cell phone inside. They knocked on the door, were let in and—voilà!—found Raymond Lambis along with drugs and drug paraphernalia. Lambis was arrested, and he moved to suppress the evidence obtained in the search. Judge Pauley granted the motion, holding that the use of the TriggerFish violated the Fourth Amendment. He likened the case to *Kyllo v. United States*, 533 U.S. 27 (2001), in which the Supreme Court disallowed the use (without a warrant) of a thermal-imaging device to determine whether a homeowner was growing marijuana plants. The Supreme Court had held that "[w]here . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." Judge Pauley also refused to get "mired in the Serbonian Bog of circuit splits" about the law of canine sniffs, which the government suggested might be likened to the use of a TriggerFish.

SEC Administrative Proceedings Get a Bit Friendlier for Respondents

The Securities and Exchange Commission (SEC) unanimously adopted final rules governing its internal, administrative proceedings. "The amendments to the Commission's rules of practice provide parties with additional opportunities to conduct depositions and add flexibility to the timelines of our administrative proceedings, while continuing to promote the fair and timely resolution of the proceedings," said SEC Chair Mary Jo White. The new rules will govern proceedings that begin on or after the rules' effective date, which will be 60 days after publication in the Federal Register. The SEC's press release is here.

Warren vs. White

Senator Elizabeth Warren, D-Mass., wrote SEC Chair White "to renew [her] objections to any efforts by the [SEC] to limit disclosure requirements in ways that would harm investors." Senator Warren blasted the SEC regarding its focus "on changing SEC rules to permit publicly traded corporations to disclose less information to their investors and the public." Senator Warren expressed her "deep[] concern[]" about the time and resources spent by the SEC on this endeavor "without a clear congressional directive, while simultaneously failing to finalize congressionally mandated rules under the 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act." Senator Warren also expressed her concern that the SEC has couched these efforts as "pro-investor" and as solving "'information overload'—a problem that the Commission has never been able to document and that analysts have described as a 'myth.'" In closing, she also lambasted the SEC as having "defied the will of Congress and its mission to protect investors and instead has pursued an agenda aligned with the narrow interests of the U.S. Chamber of Commerce and big business." Around the same time, the SEC issued proposed rules relating to "Disclosure Update and Simplification."

DOJ Gets to Keep Its Playbook Secret

The D.C. Circuit held in *National Association of Criminal Defense Lawyers v. Executive Office for United States Attorneys* that the internal Department of Justice (DOJ) publication known as the Federal Criminal Discovery Blue Book was exempt from disclosure under the Freedom of Information Act (FOIA). The circuit affirmed the district court's ruling, which we reported on here. The Blue Book "contains information and advice for prosecutors about conducting discovery in their cases, including guidance about the government's various obligations to provide discovery to defendants." While the Blue Book was not prepared for any particular litigation, the court concluded it was still protected by attorney work-product privilege because it was "prepared entirely for use in wholly foreseeable (even inevitable) litigation" and served an "adversarial function." As a result, the agency is not obligated to provide it in response to a request under FOIA.

Authors

Helen Harris
Partner

Stamford, CT | (203) 977-7418

hharris@daypitney.com

Mark Salah Morgan
Partner

Parsippany, NJ | (973) 966-8067

New York, NY | (212) 297-2421

mmorgan@daypitney.com

Stanley A. Twardy, Jr.
Of Counsel

Stamford, CT | (203) 977-7368

satwardy@daypitney.com