February 3, 2017

White Collar Roundup - February 2017

Second Circuit Refuses En Banc Review of Data-Storage Subpoena

The U.S. Court of Appeals for the Second Circuit denied the government's petition for rehearing en banc in *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*. As we reported here, the issue arose when law enforcement personnel obtained a search warrant pursuant to the Stored Communications Act (SCA) for certain e-mails housed on Microsoft's web-based e-mail system. It turns out the e-mails were stored in Dublin, Ireland. As a result, Microsoft moved to quash the subpoena. The district court denied the motion, but a panel of the Second Circuit held that the SCA did not apply extraterritorially and quashed the subpoena. The government sought rehearing en banc. By an equally divided court, the hearing was denied. Judge Susan Carney, who was on the panel, wrote a concurring opinion, defending the panel's opinion from the dissenters. Judge Carney acknowledged that the SCA is an antiquated statute that desperately requires updating but reasoned that the court's duty is to apply the statute as written, which here requires quashing the subpoena. Judges Dennis Jacobs, José Cabranes, Reena Raggi and Christopher Droney each filed a dissent from the denial, taking the opportunity to articulate why in their view the panel opinion was wrong. Judge Cabranes' dissent was particularly biting, noting that when "a decision of our court has unnecessarily created serious, on-going problems for those charged with enforcing the law and ensuring our national security, and where a legislative remedy is entirely speculative, we should not shirk our duty to interpret an extant statute in accordance with its terms." Judge Cabranes called on "a higher judicial authority" or the Congress to rectify "the panel's misreading of this important statute." Perhaps, taking his advice, the government will petition for certiorari or Congress will act. Stay tuned.

D.C. Circuit Again Reins in SEC's Attempts at Retroactive Bar

The D.C. Circuit held in *Bartko v. SEC* that the agency overstepped its authority in imposing a lifetime ban on petitioner Gregory Bartko. Between 2004 and 2005, Bartko engaged in securities fraud. After his criminal conviction for conspiracy, selling unregistered securities and mail fraud, the U.S. Securities and Exchange Commission (SEC) brought an administrative proceeding against him. There, the SEC "permanently barred Bartko from associating with six classes of securities market participants." The Dodd-Frank Wall Street Reform and Consumer Protection Act, passed in 2010, authorizes the SEC to impose both direct and collateral bars for securities-market participants. A direct bar ties the penalty to the same class of participants (e.g., barring a mischievous broker-dealer from associating with a broker-dealer); a collateral bar does not (e.g., barring a mischievous broker-dealer from associating with an investment adviser). Before Dodd-Frank, the SEC was not allowed to impose collateral bars and was not allowed to bar association with municipal advisers and rating organizations. On appeal, Bartko argued the collateral bars and the bars for the additional two classes of market participants were "impermissibly retroactive" because his conduct occurred before Dodd-Frank's passage. As we reported here, the D.C. Circuit ruled on a similar issue in *Koch v. SEC*, 793 F.3d 147 (D.C. Cir. 2015). There, the SEC barred Donald Koch from associating with municipal advisers and rating organizations, even though those classes of participants were added after his conduct concluded. In *Bartko*, the SEC endeavored to escape the reasoning and holding of *Koch*, but to no avail.

Data Breaches. Data Breaches. Data Breaches.

According to the Identity Theft Resource Center (ITRC), last year saw a 40 percent increase in data breaches over 2015. According to its website, the ITRC "is a non-profit organization established to support victims of identity theft in resolving their cases, and to broaden public education and awareness in the understanding of identity theft, data breaches, cyber security, scams/fraud and privacy issues." It reported that in 2016, the business sector experienced the highest number of data breaches yet. And for the eighth consecutive year, the leading cause of data breaches was "hacking/skimming/phishing

attacks," accounting for 55.5 percent of the overall number of breaches. The ITRC noted that "many were a result of CEO spear phishing efforts ... in which highly sensitive data, typically information required for state and federal tax filings, was exposed." The second most common were breaches that involved "accidental email/internet exposure of information," and the third was "employee error." The report concludes by noting "that several large scale breaches in 2016 – which only involved usernames, passwords, or emails ... did not specify the vast number of records exposed because this type of information does not typically trigger most data breach notification laws." For a copy of the report, click here.

Burning Question to Be Answered: Does Disgorgement Equal Forfeiture?

The Supreme Court granted certiorari in *Kokesh v. SEC* to determine the applicable statute of limitations for disgorgement orders. Under 28 U.S.C. § 2462, any "action, suit or proceeding for the enforcement of any civil fine, penalty, or forfeiture, pecuniary or otherwise, shall not be entertained unless commenced within five years from the date when the claim first accrued." Missing from that list is "disgorgement," and the question presented in *Kokesh* is whether "the five-year statute of limitations in 28 U.S.C. § 2462" applies to such claims. In the case, the SEC brought an enforcement action in October 2009 against Charles Kokesh for violating certain securities laws between 1995 and 2006. The jury found for the SEC, and the agency sought a civil monetary penalty of $5 million and disgorgement of $34.9 million. The district court ruled that some of the conduct was outside the limitations period, and it imposed a civil monetary penalty of only $2.4 million. When it came to disgorgement, the district court noted that the five-year limitations period should apply but recognized that Tenth Circuit precedent held otherwise; therefore, it imposed the full $34.9 million. On appeal, the Tenth Circuit affirmed, and Kokesh petitioned for certiorari. In his petition, Kokesh noted that the Tenth Circuit's view is consistent with that of the First Circuit and the D.C. Circuit but conflicts with the Eleventh Circuit. It urged the Supreme Court to resolve the split, which the Court agreed to do. To read the briefs regarding certiorari, click here.

SEC and FINRA Release Exam Priorities

The SEC announced its 2017 exam priorities. Areas of focus include electronic investment advice, money market funds and financial exploitation of senior investors. The priorities also reflect a continuing focus on protecting retail investors, including individuals investing for their retirement, and assessing marketwide risks. For the priorities, click here. The Financial Industry Regulatory Authority (FINRA) also released its exam priorities, which are listed here. They include firms' hiring and monitoring of high-risk/recidivist brokers; senior investors; product suitability, including excessive concentration; supervisory practices; and record retention with respect to social media and electronic communications, cybersecurity, and anti-money laundering.

Investigation Leaks Yield Investigation of Agent

A strange thing happened on the way to the indictment of William Walters. During the grand-jury investigation leading up to it, both *The New York Times* and *The Wall Street Journal* ran stories about the investigation. The stories ran in 2014, and the indictment was not returned until 2016. In September 2016, Walters filed a motion arguing that the prosecution team violated Federal Rule of Criminal Procedure 6(e), which requires secrecy of grand-jury proceedings. The U.S. Attorney's Office for the Southern District of New York (USAO) responded to the motion, but the court ordered a hearing. When preparing for the hearing, the USAO learned an FBI agent had, in fact, leaked information to the press. Upon learning this information, the USAO filed two letters with the court: The first explained the procedural history and recommended a way forward; the second was an ex parte letter filed under seal with more detailed information about the USAO's investigation. Both letters were filed in December 2016. In January 2017, the leaker communicated his agreement to lift the seal on the second letter, which was publicly filed. The leaking agent was FBI Coordinating Supervisory Special Agent David Chaves, who now faces investigations by the FBI Office of Professional Responsibility and the Office of the Inspector General for the Department of Justice. As for the prosecution of Walters, the USAO advised the court it could not conclusively determine whether a Rule 6(e) violation had occurred. As a result, it suggested that the court assume such a violation and "proceed to consider the issue of remedy" as approved in *In re Sealed Case*, 151 F.3d 1059, 1068 (D.C. Cir. 1998).

Deputizing the Geek Squad

What happens when someone sends a computer to Best Buy's Geek Squad for repairs and the computer contains contraband? Defendant Mark Rettenmaier is about to find out. He hired Best Buy to repair his computer, and its Geek Squad team in Kentucky found images of child pornography on it. They notified the FBI, and Rettenmaier was indicted for violations

of federal law. But Rettenmaier filed a motion to suppress the evidence, arguing that when they searched his computer, the Geek Squad team members were acting as agents of the FBI. It turns out that the FBI has cultivated relationships with about eight members of the Geek Squad team, paying them for providing information about contraband they find on computers. The issue, currently pending before U.S. District Judge Cormac Carney in the Central District of California, is the question of whether the Geek Squad "search" violated Rettenmaier's rights. Rettenmaier argues it did because the members of the Geek Squad, who otherwise would not be subject to Fourth Amendment limitations, were acting as agents for the FBI. If Judge Carney agrees, he might suppress the evidence against Rettenmaier because the Geek Squad did not have a warrant to search his computer. For an article about this case, click here.

Old Statutes and IP Larceny: The Confusion Continues

A New York appellate court has weighed in on the convoluted case of former Goldman Sachs computer programmer Sergey Aleynikov. Or more precisely, *two* intertwined cases, one still pending in New York and an earlier one upended in 2012 by the Second Circuit. Together, the state and federal cases exemplify the bad fit between criminal statutes drafted in an earlier era and intellectual property theft in the current, digital age. In both matters, Aleynikov was indicted for having covertly copied source code for Goldman Sachs' high-frequency trading platform to an overseas server, which he gave to his new employer. In 2010, Aleynikov was convicted after a trial in the Southern District of New York on charges that included violating the National Stolen Property Act (NSPA), 18 U.S.C. § 2314. The Second Circuit vacated that conviction two years later in *United States v. Aleynikov*, 676 F.3d 71 (2d Cir. 2012). The NSPA proscribes interstate trading or trafficking in stolen *tangible* "goods." In the Second Circuit's view, the copies Aleynikov made of the source code were intangible and accordingly outside the NSPA's ban. Later in 2012, the Manhattan district attorney charged Aleynikov with violating a 1967 statute proscribing the wrongful taking of "secret scientific material" by making "a tangible reproduction." In 2015, Aleynikov was convicted following a state court trial. Later the same year, the trial court granted Aleynikov's motion to dismiss the indictment. In an unusually long (57-page) opinion, the trial court held that the copying of the source code created an intangible item that New York law does not reach. But the First Department squarely disagreed and reinstated Aleynikov's conviction. The court held that "by copying the source code to the overseas server, Aleynikov made a "tangible *reproduction* of" the code and therefore "unquestionably" violated the state statute. Aleynikov apparently intends to appeal. Accordingly, his circuitous path through the courts – and gray areas of the law – may well continue.

Authors



Helen Harris
Partner

Stamford, CT | (203) 977-7418

hharris@daypitney.com



Stanley A. Twardy, Jr.
Of Counsel

Stamford, CT | (203) 977-7368

satwardy@daypitney.com