December 5, 2016

White Collar Roundup - December 2016

The Plain View Doctrine in the Age of the iPhone

U.S. District Judge Kevin McNulty of the District of New Jersey ruled in *United States v. Ravelo* that agents lawfully searched defendant Keila Ravelo's iPhone, which they seized at the time of her arrest. When Ravelo was a partner at a law firm in New York, the government began to investigate her for fraud and tax evasion. Government agents obtained an arrest warrant, which they executed at Ravelo's home. During her arrest, Ravelo picked up her iPhone and typed in a code to unlock it. One of the agents told Ravelo she could not make any calls, but would allow Ravelo to obtain her attorney's phone number and provide it to her son. Without then obtaining the number, Ravelo locked the phone. The agent then picked up the phone and asked Ravelo for the code to allow the agent to provide the attorney's phone number to Ravelo's son. Ravelo gave the agent the code and the agent unlocked the phone. Upon doing so, the screen showed the email program with an email to or from Gary Friedman, who the agent knew to be a possible co-conspirator. The agent did not open the email, but pressed the home button and followed Ravelo's prompts to find her attorney's phone number. The agents kept the phone and obtained a warrant to search its contents. Ravelo moved to suppress the evidence obtained from the phone, claiming the agents unlawfully seized it. Judge McNulty disagreed. He reasoned that the agents lawfully obtained Ravelo's consent to unlock the phone and then viewed the incriminating email in "plain view" upon doing so. That observation did not impinge on Ravelo's Fourth Amendment rights and formed a lawful basis to obtain a warrant to search the phone. As a result, Judge McNulty denied the motion to suppress, and the government may use the fruits of their search against Ravelo at trial.

Urging the Second Circuit to Hold Prosecutors to Account

"In many respects, this case is extraordinary." So begins the *amicus curiae* brief filed by the National Association of Criminal Defense Lawyers (NACDL) in *Ganek v. Leibowitz*, currently pending in the U.S. Court of Appeals for the Second Circuit. The plaintiff-appellee in the case, David Ganek, sued several law enforcement officers, several assistant U.S. attorneys in the Southern District of New York and Preet Bharara, the U.S. Attorney in that district. Ganek claims that those officials violated his civil rights when they fabricated information in an affidavit to obtain a search warrant. As reported here, District Judge William H. Pauley III partially denied the defendants' motion to dismiss, and they appealed. In its *amicus* brief, the NACDL urged the Second Circuit to affirm the ruling. It argued the case was "extraordinary" because law enforcement agents rarely "admit to the existence of a false statement in a search warrant affidavit," targets of criminal investigations rarely "strike back at the prosecutors with a civil rights lawsuit" and U.S. Attorneys rarely are "alleged to be so directly involved in the allegations underlying a civil rights lawsuit." Even so, the NACDL argued, "[m]isconduct by prosecutors and other law enforcement officers — including the problem of false statements in search warrant affidavits — is rampant." In that way, it claimed, the case "raises an issue that is far too common."

Using Cell-Site Simulators to Catch Crooks

In a contentious and split decision, the Seventh Circuit in *United States v. Patrick* brushed aside privacy concerns and affirmed the conviction of Damian Patrick, who argued that his arrest, which was effectuated with the use of a cell-site simulator (or Stingray), was unlawful. Judge Frank Easterbrook wrote the majority opinion, beginning it by explaining that "[p]olice in Wisconsin arrested Damian Patrick while he was in a car on a public street and found him armed." At the time, Patrick was on parole but had not complied with the conditions of release, which resulted in the issuance of an arrest warrant. Police obtained a second warrant to use cellphone data to find him. Judge Easterbrook noted that police are allowed to use a warrant "to get evidence to locate a wanted person." They also can arrest someone in a public place without a warrant, as long as they have probable cause to do so. Patrick claimed, however, that the arrest was invalid because the police, who sought a warrant only for cellphone data, used a Stingray without notifying the judge. The court dismissed this argument, noting, "[q]uestions about whether use of a simulator is a search, if so whether a warrant authorizing this method is essential, and whether in [a] particular situation a simulator is a reasonable means of executing a warrant, have yet to be addressed by any United States court of appeals," so it was "best to withhold full analysis until these issues control the outcome of a concrete case." Chief Judge Diane Wood dissented. To her, the case "raises serious issues about the use of cell-site simulators to track down the location of a target person." She accused her colleagues of underestimating the "relevant technology's capabilities" and noted this was "the first court of appeals case to discuss the use of a cell-site simulator," largely because the government often withdraws evidence that relies on it. To her, the court should have taken a harder look at the invasiveness of such devices. We did so here.

SEC Dodd-Frank Whistleblower Report: The End of an Era?

In what might be the last such report, the U.S. Securities and Exchange Commission (SEC) issued its 2016 Annual Report to Congress on the Dodd-Frank Whistleblower Program. In the report, the SEC notes that in August 2016, the SEC's awards to whistleblowers "surpassed the $100 million mark" and that the program "has already awarded more than $111 million to 34 whistleblowers whose information and cooperation assisted the agency in bringing multiple successful Commission enforcement actions and related actions." The report also noted "[t]he transformative effect" of the program because it has facilitated the return of "hundreds of millions of dollars" to investors. According to the SEC, there has been a "consistent increase in the number of whistleblower tips received," which in 2016 was over 4,200 tips, "a more than 40 percent increase in whistleblower tips since FY 2012, the first year for which [the SEC has] full-year data." Perhaps speaking to the incoming administration, the report contends that "the continued payment of significant awards, like those made this past year, will continue to incentivize company insiders, market participants, and others with knowledge of potential securities law violations to come forward and report their information to the agency."

Fighting Cybercrime and Unlocking Smartphones

Manhattan County District Attorney Cyrus R. Vance Jr. lauded his office's efforts to combat cybercrime and called for access to smartphones in a speech at his office's 7th Annual Financial Crimes and Cybersecurity Symposium. Vance explained that in his view, "Cybercrime is second only to terrorism in its potential to disrupt the functioning of our society." As a result, his office, along with the other members of the Global Cyber Alliance, is offering two free products — DMARC and DNS filtering — to fight cybercrime. Vance also called on Congress to enact legislation to require smartphone makers to enable law enforcement to access data on smartphones that have been lawfully seized. He complained that the heightened security on smartphones "does nothing to protect us from the rising tide of cybercrime," which usually works because of sophisticated — or not-so-sophisticated — phishing schemes. Rather, in his view, such "device encryption" only "thwart[s] law enforcement's ability to identify the perpetrators [of cyberattacks] and take them out of the game," and prevents law enforcement from using

evidence residing on smartphones against other white collar and street-level defendants. He recommended his office's report on the issue, which is available here.

Encryption Principles

In the same vein, BSA | The Software Alliance issued its Encryption Principles: A Comprehensive Approach to Promoting Global Cybersecurity, Public Safety, Personal Privacy & Prosperity. That document offers eight "Principles for Action" on the subject: improving data security, enhancing law enforcement capabilities, promoting privacy, protecting confidential government information, encouraging innovation, defending critical infrastructure, understanding the global impact and increasing transparency. Undoubtedly, this debate will continue.

As Predicted …

We reported last month on defendant Michael Rand's petition for certiorari to the U.S. Supreme Court. That petition raised two issues: one regarding a defendant's ability to obtain pretrial discovery and one regarding the principles of loss causation in a criminal securities case. We noted that a cert. grant would be a long shot, and it was: the Supreme Court denied the petition on November 28.

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