BARNES & THORNBURG LLP

Corporations And Unreasonable Searches And Seizures: Does The Supreme Court's Decision In Riley V. California Signal The Rebirth Of The 4th Amendment In White Collar Cases?

July 18, 2014 | | Case To Watch,The GEE Blog

There has been much attention paid to the Supreme Court's recent decision in *Riley v. California*, Nos. 13-132 and 13-212 (June 25, 2014), and justifiably so. It was notable because it was a 9-0 decision in a criminal case – a rare occurrence in the Supreme Court's history, especially for this deeply-divided Court. But it was also an important, landmark ruling for the Fourth Amendment and its protections against unreasonable searches and seizures. In its narrowest interpretation, the Supreme Court's decision in *Riley* rejected the argument made by law enforcement that cell phones could be searched without a valid warrant if they were seized at the time of arrest. The Supreme Court has repeatedly recognized that there are appropriate exceptions to the Fourth Amendment's warrant requirement, perhaps the most prominent of which is the exception that allows an officer to search a person's body at the time of their arrest. Law enforcement unsuccessfully argued that a cell phone, found on an arrestee's person, could likewise be seized and its contents searched at the time of the arrest under this well-established Fourth Amendment exception. Corporations cannot be arrested and do not have "bodies" to be searched. Chief Justice Roberts' opinion in *Riley* makes no mention of the application of the Fourth Amendment to corporations or more broadly, to white collar criminal cases in general. Therefore, few have suggested that *Riley* will alter the way corporations are investigated for white collar crimes in any material way. And perhaps they are right, but *Riley* is important for more than its holding. The Supreme Court has long held that "[t]he Warrant Clause of the Fourth Amendment protects commercial buildings as well as private homes." *See Marshall v. Barlow's Inc.*, 436 U.S. 307 (1978). Businesses, like individuals, have certain privacy expectations, and businessmen, like the occupants of a residence, have "constitutional right[s] to go about [their] business[es] free from unreasonable official entries upon [their] private commercial property." *Id.*. The Supreme Court made clear that its decision to place clear limits on the seizure of cell phones in *Riley* was not because they are "phones," but rather because "these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone." That conclusion, and more importantly, the Court's nuanced articulation of what these "minicomputers" are capable of performing is what is so striking and important. The Supreme Court recognized that smart phones have on average "33 apps" that could range from apps for "Democrat Party news and Republican Party news" to "apps for alcohol, drug, and gambling addictions" to "apps for buying or selling just about anything, and the records of such transactions" too. Quite simply, the Supreme Court, stated that a cell phone is "a digital record of nearly every aspect of [individuals'] lives – from the mundane to the intimate." Invoking the great jurist Learned Hand, Justice Roberts analogized that searching a suspect's person is totally different "from ransacking his house for everything which may incriminate him," which is what occurs when the Government searches a person's cell phone. Yet that is exactly how modern white collar criminal

RELATED PRACTICE AREAS

Financial and Regulatory Litigation
Government Litigation
Securities and Capital Markets
White Collar and Investigations

RELATED TOPICS

Corporations

investigations of corporations are conducted – they constitute a virtual "ransacking" of a business, where warrants typically authorize the search and seizure of every phone, desktop, tablet, hard drive, flash drive, and laptop in that business. Of course, that gives investigators access to every data point of information contained (or previously contained) on those devices – regardless of whether the subject matter of all of that information even remotely relates to the subject matter for which a magistrate found probable cause to issue that search warrant in the first place. Investigators are not permitted to grab and seize hard copy files that are clearly unrelated to their investigation and outside the scope of the warrant, so why should they be permitted to do so with electronic files? *Riley* could finally lay the groundwork to require investigators to more precisely and with greater particularity identify the electronic records they are allowed to seize. Rather than being allowed to indiscriminately seize and review every email and text message, is the day coming when investigators will be required to identify the electronic files and records by subject matter, rather than just be the type of device where those items are stored? *Riley* also recognizes that technology allows users to remotely store information far beyond the microchips in these "minicomputers" themselves. What was perhaps most interesting was the Supreme Court's discussion of "cloud computing" and the "capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself." Certainly the drafters of the Fourth Amendment could never have envisioned its application to "cloud computing" or the fact that "the same type of data may be stored locally on the device for one use and in the cloud for another." Defense attorneys need to be prepared to recognize and challenge the same potential weaknesses in warrants for businesses. As the Supreme Court points out, "the search incident to arrest exception may not be stretched to cover a search of files accessed remotely – that is, a search of files stored in the cloud." However, "officers searching a phone's data would not typically know whether the information they are viewing was stored locally at the time of the arrest or has been pulled from the cloud." Likewise, warrants may often call for the seizure of electronic devices, but not the remote storage systems or even the centrally-controlled networks where the information is actually maintained. The right to seize and search a device should not give rise to the right to search and seize a separate storage unit, located in a different physical location that is not covered by the warrant. Fourth Amendment caselaw is typically very favorable to the Government, and many worried that the *Riley* decision would be yet another expansion of the Government's investigative authority. While this subject matter was clearly new territory for the Supreme Court, white collar attorneys and their corporate clients should take some heart in the decision. The Supreme Court got it – that is they took the time to understand just how truly transformative technology is and how technology impacts the way individuals now operate. We should be encouraged by that fact. In fact, all nine justices – regardless of political background or judicial philosophy -- recognized the radical implications of creating broad exceptions to the Fourth Amendment for electronic devices and data and information. Given the fact that the constitutional right to corporate privacy is indiscriminately violated everyday by sweeping, imprecise warrants of corporations, their offices, and the electronic data contained therein, *Riley* could indicate that the Fourth Amendment may yet have new life in corporate boardrooms as well, which may also limit the way white collar investigations are conducted.