Privacy, Technology, and the Fourth Amendment

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

December 15, 1791

Applies to government action, not non-governmental entities.

Burdeau v. McDowell, 256 U.S. 465 (1921) (Prosecution could retain and use papers stolen by private parties)

A. The Third-Party Doctrine

"[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."

United States v. Miller, 425 U.S. 435, 443 (1976) (Upheld use of USAO subpoenas to bank to produce copies of depositor's records – no intrusion into any constitutionally protected area)

"[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."

Smith v Maryland 442 U.S. 735, 741(1979) (upheld warrantless installation of a pen register at a phone company office to record numbers dialed by defendant from his home upheld – he had no reasonable expectation of privacy in numbers he "voluntarily" conveyed to the phone company)

B. Expectation of Privacy

Traditionally a “search” meant a government actor’s physical intrusion into a constitutionally protected area.

Olmstead v. United States, 277 U.S. 438 (1928) (Upheld warrantless wiretapping - no trespass by officers onto defendant’s property); *United States v. Jones*, 565 U.S. 400 (2012) (Justice Scalia: Installation of GPS device on suspect’s Jeep to track him for 28 days was a search. There was physical intrusion into the Jeep. Justice Sotomayor concurs but says that the third party doctrine is “ill-suited to the digital age.”)

Katz v. United States, 389 U.S. 347, 353 (1967).

Eavesdropping by an electronic listening device placed on the outside of a telephone booth -- a location not within the "persons, houses, papers, and effects" that the Fourth Amendment protects against unreasonable searches. The Court held that the Fourth Amendment protected Katz from the warrantless eavesdropping because he "justifiably relied" upon the privacy of the telephone booth. *Id.* at 353. As Justice Harlan said in his concurrence, a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.

“It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.”

Justice Antonin Scalia in *Kyllo v. United States*, 533 U.S. 27, 33-34 (2001) (Agent’s use of thermal imaging device, not in general use, while seated in a car on a public street to scan interior of home to detect high-intensity lamps consistent with marijuana grow, was a “search” and was presumptively unreasonable without a warrant.)

Riley v. California, 134 S. Ct. 2473 (2014). Held that absent exigent circumstances warrantless searches of cell phones seized incident to arrest violated the Fourth Amendment.

"Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life," …. The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant."

Riley v. California, 134 S. Ct. at 2494-2495, Chief Justice Roberts (citation deleted).

C. Carpenter v. United State, 138 S. Ct. 2206, June 22, 2018

Facts in *Carpenter*

A cooperating suspect in a series of Radio Shack and T-Mobile store robberies in Michigan and Ohio gave investigators cell phone numbers of his 15 alleged accomplices. Pursuant to the Stored Communications Act (SCA) prosecutors obtained court orders to obtain from wireless carriers MetroPCS and Sprint cell site locator information (CSLI) for Timothy Ivory Carpenter and others. The SCA enables the government to get such records when it "offers specific and articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation." The government obtained over 12, 000 location points recording the whereabouts of Carpenter's phone over 159 days. At trial an FBI agent produced maps showing that the phone was near four

of the six charged robberies. Carpenter was convicted, sentenced to over 100 years, and appealed.

The Sixth Circuit Court of Appeals affirmed on the ground that Carpenter had no reasonable expectation of privacy in the CSLI i because he had shared that with his wireless carriers.

The Opinions in *Carpenter*,

Chief Justice Roberts' Majority Opinion

The case lies at the intersection of the physical intrusion/ surveillance line of cases (like *United States v Knotts*, 460 U.S. 276 (1983), which upheld use of a beeper in a planted container to track a suspect's physical movements, and *Jones*) and the third party cases (like *Miller* and *Smith*). The majority declined to apply the third party doctrine and held that cell phone users have a reasonable expectation of privacy in CSLI. CSLI is a far cry from ordinary business records. As the Court said in *Riley*, cell phones, like other digital devices, have come to play a pervasive and indispensable role in daily life. They contain gigabytes of personal information, which knowledgeable users try to protect. Digital technology has made it possible to track a wireless user's location history for as long as the carrier preserves its records. In no realistic sense does the cell phone user voluntarily entrust her or his location to their carrier. Chief Judge Roberts writes,

> "We decline to grant the state unrestricted access to a wireless carrier's database of physical location information. In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection. The Government's acquisition of the cell-site records here was a search under that Amendment."

138 S. Ct. at 2223

The SCA authorized the issuance of a subpoena for CSLI upon a showing of reasonable suspicion, not probable cause.

The majority opinion is narrow. It reiterates that the government remains able to subpoena third party records on less than probable cause in the overwhelming majority of investigations and that exigent circumstances such as fact-specific threats or ongoing emergencies can justify warrantless seizure of CSLI as being objectively reasonable under the Fourth Amendment. The Court expresses no view on downloads of information on all the devices connected to a particular cell site during a particular time interval, nor does it overrule *Smith* and *Miller*, nor does it question conventional surveillance techniques such as surveillance cameras, nor does it consider data collection involving foreign affairs or national security.

Justice Kennedy's Dissent

Justice Kennedy would apply the Third Party Doctrine to CSLI records and notes that none of the CSLI in this case covered less than 7 days so that the majority holding would not preclude a subpoena of cell-site records covering six days or less. The investigators did not search anything of Carpenter's. The subpoenas in this case complied with the Fourth Amendment reasonableness requirement because they were "sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance [was not] unreasonably burdensome." The justice notes that Fourth Amendment's applicability to contemporary equivalents of an individual's own "papers" or "effects" even when held by a third party and cites a Sixth Circuit case which held that a defendant had a reasonable expectation of privacy in his e-mails retained by his internet service provider so that they should not have been obtained absent a warrant based on probable cause. (The

exclusionary rule did not apply because the agents relied in good faith on the SCA.). Given the changes in technology and the Fourth Amendment standard of reasonableness, the Court should defer to legislative judgment, as in the SCA, on balancing personal privacy against the needs of law enforcement. Justice Kennedy bemoans the questions raised by the majority opinion. The majority does not explain what makes records a distinct category of information. Are bank records distinct from credit card records? Are cell phone records distinct from landline records? "The Court's multifactor analysis-considering intimacy, comprehensiveness, retrospectivity, and voluntariness – puts the law on a new and unstable foundation." 138 S. Ct. at 2234. The majority does not explain how much information must be presented to support a warrant. What about IP addresses or website browsing history? Justice Kennedy concludes his jeremiad as follows:

> "[B}y invalidating the Government's use of court-approved compulsory process in this case, the Court calls into question the subpoena practices of federal and state grand juries, legislatures, and other investigative bodies, as Justice Alito's opinion explains …. Yet the Court fails even to mention the serious consequences this will have for the proper administration of justice.

Carpenter v. United States, 138 S. Ct. at 2234 (Citation omitted)

Justice Thomas' Dissent

Justice Thomas urges the Court to reject the reasonable expectation of privacy test. Whether an expectation of privacy is "reasonable" is a judgment about policy, not law. A particular expectation of privacy is reasonable if the majority of the Court says it is. Justice Thomas opines that *Katz* has no basis in the history or text of the Fourth Amendment. Since the records in this case belonged to the

wireless carriers, not Carpenter, he was not subject to a search and his constitutional rights were not violated.

Justice Alito's Dissent

Justice Alito opines that the majority's treatment of an order to produce like an actual search is "revolutionary" and unless restricted to the facts of the present case could require every grand jury subpoena *duces tecum* to be supported by probable cause. Carpenter had no Fourth Amendment property rights in the CSLI records generated by his wireless providers.

Justice Gorsuch's Dissent

Justice Gorsuch wonders what is left of the Fourth Amendment and recognizes that in the digital age "we use the Internet to do most everything."

> Even our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third party servers. *Smith* and *Miller* teach that the police can review all of this material, on the theory that no one reasonably expects any of it will be kept private. But no one believes that, if they ever did."

Carpenter v. United States, 138 S. Ct. at 2262. Justice Gorsuch discredits *Smith* and *Miller* as, "A doubtful application of *Katz* that lets the government search almost whatever it wants whenever it wants."

138 S. Ct. at 2264. He criticizes the *Katz* "reasonable expectation of privacy" approach for the much same reasons as Justice Thomas. It is amorphous, not tethered to the text and history of the Fourth Amendment, and relies on the intuition of unelected judges to determine what expectations of privacy society considers reasonable.

Justice Gorsuch proposes what he describes as a third approach which rests on common law, particularly property law, and on federal and state statutes. The Fourth Amendment protects the houses, paper or effects that are yours. However under his "more traditional approach" Fourth Amendment protections for your papers and effects do not disappear because you share them with someone else who like a traditional bailee owes you the duty to keep them safe. Your internet service provider should have the same obligation to keep your e-mails private as the traditional letter carrier. Just because you have to entrust a third party with your data does not mean that you lose all Fourth Amendment protections in it, as when the police impound your car. Moreover, federal and State legislators can enact statutes creating property rights in intangible digital assets, which rights would then be protected by the Fourth Amendment. Although Carpenter could have relied on federal statutes, such as 47 U.S.C. § § 222 & 207, as giving him a protected right to control his cell-site data, his failure to raise and preserve that issue should have doomed his appeal.

Bjorn Lange

Assistant Federal Public Defender

Concord, NH 03301