# Symposium: Granular analysis versus doctrine in *Carpenter*

Jim Harper

August 1, 2017

The outcome of *Carpenter v. United States* will turn on how granular the Supreme Court is in analyzing what happens when government agents require telecommunications providers to disgorge data about their customers. If the court carefully thinks through the application of the Fourth Amendment to cell site location information (CSLI) sought by the government – if the court treats it as a careful legal exercise – the result will be good for privacy and for the administration of the Fourth Amendment. If the court retreats to doctrine and examines the case in terms of "reasonable expectations of privacy," the outcome and value of the case will be less clear.

Recent Fourth Amendment history offers examples to illustrate the difference between fuzzy and granular analysis.

The corner of 8th and C Streets, NE, in Washington is a 10-minute walk from the Supreme Court – past million-dollar homes on leafy, tree-lined streets. It was a different neighborhood in 1968, when Willie Robinson was arrested there for driving without a license.

Officer Richard Jenks had recognized Robinson, and knew he didn't have a license. Jenks pulled Robinson over, arrested him and searched him incident to arrest. Finding a crumpled cigarette pack in Robinson's breast pocket, Jenks searched it and discovered heroin capsules. The government charged Robinson, and he was convicted of "possession and facilitation of concealment of heroin."

Robinson challenged that conviction all the way to the Supreme Court – seven blocks away.

The contents of a cigarette pack can't be evidence of a driving infraction, and, once removed from an arrestee, they cannot present a danger to officers. But in *United States v. Robinson*, the Supreme Court approved searches of things arrestees carry. That may have seemed pragmatic, but it didn't follow the clean lines of justification for searching arrestees: the possibility that evidence might be destroyed or officers put in danger.

*Robinson* gave rise to a Fourth Amendment "container" doctrine, which lower courts and later decisions made more and more permissive. The Supreme Court had to return to the issue several times to shut the container doctrine down, in cases such as 1977's *United States v.*

*Chadwick* and *Arizona v. Gant* in 2008. The court clearly declined to treat cellphones as "containers" in its 2014 *Riley v. California* decision.

It turns out that Justice Thurgood Marshall had it right when he dissented in *Robinson*. Marshall carefully analyzed the context of the stop and each step in the arrest and search of Robinson. The typical arrest is a series of seizures and searches, each of which may have different legal justifications – and all of which must have at least one.

"It does not appear that Jenks had any reason to believe, or did in fact believe, that the [cigarette pack and its contents] were weapons of any sort," Marshall wrote. "He nevertheless opened up the package and looked inside." Thus, Marshall undercut the only valid cause for the search the majority might have assumed.

A granular analysis of the type Marshall performed in *Robinson* is likely to produce a solid opinion in *Carpenter*. But if the Supreme Court glosses over the technical details present in *Carpenter*, it will probably produce another *Robinson*: flabby doctrine that requires later correctives.

The trick is to apply the Fourth Amendment as a law, eschewing doctrines like the "reasonable expectation of privacy" test. The court should ask:

- Was there a seizure?
- Was there a search?
- Was any search or seizure of "persons, houses, papers, [or] effects"?
- Was any such search or seizure reasonable?

Careful readers will note that the Fourth Amendment lists searches first and then seizures. The order of the inquiry is better reversed because seizures so often precede searches or constitute them. The first question to ask is whether a given fact pattern included any seizure.

Fourth Amendment doctrine stands in the way of that very first step in the analysis. It lumps seizure and search together, treating them as the same: a search. And it suggests that there is no "search" when government agents acquire data about someone from a third party.

But the "third-party doctrine" as found in *Smith v. Maryland* is itself a derivative of reasonable-expectations doctrine, which the justices have used more sparingly – and almost never as the majority's decision rule – for a couple of decades. The intimate data reflecting our cell-phone usage should probably not be governed by a 1970s case dealing with the land-line calls of one person whose criminal behavior was established by good evidence.

What actually happens when the government takes data such as CSLI from a third-party communications provider is best characterized as a seizure.

CSLI is held subject to contractual protections, such as the provider's terms of service and privacy policy. These are the "metes and bounds" of the property rights customers have in the data. Generally, customers retain the right to exclude all others from accessing the data, except

for a limited class of service providers and other parties under specific conditions. The contract also reflects what rights to use or sell information the provider owns.

There are parallel regulations that accord property rights in data, if tacitly. But the Federal Communications Commission's regulations relating to telecommunications data tellingly refer to it as "Customer Proprietary Network Information."

There is an argument that terms of service and privacy policies deny customers the right to exclude others from data that is disclosed "to a governmental entity to comply with valid legal process, such as warrants, court orders or subpoenas." That begs the question whether a particular process is valid and legal. The customer should be able to argue his or her side of that question. Presuming the opposite would make surplus language of important contract terms.

Like many, the facts of this case present both a digital seizure and a search. That search occurred when the government converted the data into a form that people could perceive. As Orin Kerr wroteof the Supreme Court's 2001 thermal-imaging case, *Kyllo v. United States*, "it must be the transformation of the existing signal into a form that communicates information to a person that constitutes the search."

The next step in applying the Fourth Amendment also requires nesting modern technology into our constitutional framework. That is asking whether any seizure or search affected persons, houses, papers or effects.

It was not papers as a form-factor for cellulose that the framers of the Fourth Amendment sought to protect, of course, but the commonly used medium for storage and communication of information. Today, the federal trial court system has recognized, as it must, that digital representations of information are equivalent to paper documents for purposes of both filing and discovery.

The subject matter held in digital documents and communications is at least as extensive and intimate as what was held on paper records when the Fourth Amendment was written, and probably much more so. The storage of documents on media other than paper changes nothing about their Fourth Amendment significance. Digital data are papers.

As a circuit judge, now-Justice Neil Gorsuch treated email as constitutionally protected, inferentially but necessarily bringing it within the "papers or effects" category.

Finding that digital documents are constitutional "papers" should bring the Supreme Court to the final question: whether the seizure and search of this data was reasonable. The structure of the Fourth Amendment suggests, and the Supreme Court's precedents make clear, that getting a warrant is the reasonable thing to do when it can be done. "It is a cardinal rule that … law enforcement … use search warrants wherever reasonably practicable."

That quote is from *Chimel v. California*, the 1969 case that established the factors still used today to determine when a search incident to arrest is reasonable. The Supreme Court deviated from the *Chimel* factors in *Robinson*, and that created the container doctrine, which the court later had to correct.

If the *Carpenter* court is granular in its analysis of what actually happens to CSLI, following the model of Marshall in *Robinson*, it will come up with a clear, juridical ruling. If it retreats to broad guesses about society-wide "expectations of privacy," the result will be something different.

*Jim Harper is vice president of the Competitive Enterprise Institute. As a senior fellow at the Cato Institute, he filed an amicus brief for the institute in support of Timothy Carpenter's petition for certiorari in Carpenter v. United States.*