Privacy advocates advise Supreme Court to protect phone location data under the 4th Amendment

Devin Coldeway

August 16, 2017

Among the Supreme Court's many upcoming cases is Carpenter v. United States, which will settle the question of whether your location and movements, as determined by the ordinary interactions of your phone with the network, are protected by the Fourth Amendment. Dozens of companies, advocates, experts and interested parties just weighed in ahead of the hearing.

The issue, briefly summarized: Timothy Carpenter was convicted partly by the use of 127 days (and 12,898 individual location points) of cell site location information (CSLI) acquired by police from telecoms without a warrant. The argument that this information was protected, and that its collection constituted unreasonable search and seizure, failed to convince the Appeals court.

Just as a refresher, here's that 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.

The ACLU, which represents Carpenter in the case, already filed a brief explaining its position, but it's clear that plenty of others, from tech giants to gun owners, want to add their voices to the chorus. Here are the highlights from their Amicus Briefs, which are helpfully listed here if you'd prefer to read them in full. (I've done some minor formatting.)

Cato Institute, Competitive Enterprise Institute, et al.

The government's compulsory acquisition of data in this case was a seizure. Processing the data to make it human-readable was a search. The records were in relevant part the property of Messrs Carpenter and Sanders… And digital documents are best treated as constitutional "papers" or "effects."

There is a presumption in favor of the warrant requirement suggested by the text of the Fourth Amendment, and it is confirmed by this Court's precedents. Thus, it was unreasonable to seize

and search the data without a warrant. Lacking exigency or other excuse, the government should have gotten one.

Center for Democracy and Technology

The changes resulting from digital technology — with Americans storing vast quantities of personal information with third parties, and third parties creating databases of personal information not previously available — make it eminently reasonable to conclude that Americans have a legitimate expectation of privacy with respect to much of this information.

The Court also should recognize that whether the individual provided personal information "voluntarily" should not be accorded any weight in the reasonable-expectation-of-privacy inquiry, because there is no correlation between the voluntary provision of information to a third party and legitimate expectations of privacy. For example, individuals voluntarily transfer the contents of emails, photographs, and sensitive personal documents to third-party service providers who store this information. Yet individuals believe, correctly, that absent very unusual circumstances, this information will be private: it will not be viewed by anyone other than themselves or persons who they authorize.

EFF, Brennan Center for Justice, National Association of Criminal Defense Lawyers et al

(Note: Smith v. Maryland is a 1979 Supreme Court case that established the precedent that phone records don't require a warrant, mostly because of how analog phones worked — the data wasn't yours to control, but had been volunteered to a third party, i.e. the phone company.)

Equipped with CSLI, police can now not only place suspects at specific crime scenes, but can also reconstruct almost anyone's movements for many months in the past. Yet law enforcement obtains this type of information without a warrant, tens of thousands of times a year.

The Sixth Circuit below relied on this Court's opinion in Smith v. Maryland to hold Americans lack a reasonable expectation of privacy in CSLI because it is a business record held by third-party service providers.

But Smith cannot govern here. The now-routine use of CSLI to reconstruct individuals' movements over extended periods of time was "nearly inconceivable just a few decades ago." Whatever wisdom the so-called third-party doctrine had in 1979 when Smith was decided, it is entirely "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." The Court should instead hold that CSLI is subject to the full protection of the Fourth Amendment.

Electronic Privacy Information Center and associated experts

Smith v. Maryland arose in a world that no longer exists.

This Court has never held that the government may search and seize records of where a person travels without triggering Fourth Amendment scrutiny. Indeed, the Court recently determined in Riley that the government could not seize such sensitive cell phone data without a warrant. There is also no evidence that cell phone users expect to be subject to such routine tracking of their

private lives — quite the contrary. We as a society are not prepared to accept pervasive, warrantless location tracking as objectively reasonable.

The Court's decision in Smith does not determine the scope of Fourth Amendment protection today. In the modern era, cell phone location records provide a "comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." ...And while Congress should address the "complex subject" of location tracking by enacting a "comprehensive stature," the Court bears the fundamental responsibility of determining the appropriate scope of the Fourth Amendment.

Scholars of Criminal Procedure and Privacy

This Court should resist extending the reasoning of Smith v. Maryland — a 38-year-old case built on a faulty privacy premise — to the modern, hyper-connected, technology-dependent world. Instead, the Court should recognize that the new realities of this world require new legal doctrines to fit the privacy expectations shared by most Americans.

Criminal procedure and privacy scholars are in near-unanimous agreement that an extension of what some have called the "third-party doctrine," which holds that people lack a reasonable expectation of privacy in information voluntarily conveyed to third parties, could eliminate citizens' privacy in the modern age. Smith is grounded in a pre-digital era, and cannot support future application of the Fourth Amendment.

Pretty much every major tech company, plus Verizon, which owns Oath, which owns TechCrunch

In the digital context, inflexible doctrines that categorically foreclose any protection for data automatically generated by ordinary digital activity—or that will be generated by the yet-to-be-conceived technologies of tomorrow—are not sustainable. In particular, the analog-era notion that transmission of data to a third party is necessarily "voluntary" conduct that precludes Fourth Amendment protection should not apply in a world where devices and applications constantly transmit data to third parties by dint of their mere operation. No constitutional doctrine should presume that consumers assume the risk of warrantless government surveillance simply by using technologies that are beneficial and increasingly integrated into modern life.

Rather than adhere to rigid Fourth Amendment "on/off" switches developed in the analog context, courts should take a more flexible approach that realistically reflects the privacy people expect in today's digital environment. Consistent with the general reasonable-expectation-of-privacy inquiry, courts should focus on the sensitivity of the data at issue and the circumstances of its transmission to third parties. That approach would better reflect the realities of today's digital technologies and accommodate the technologies of the future.

Technology experts including Ashkan Soltani, Bruce Schneier, Nicholas Weaver, Scott Bradner, Susan Landau, Philip Zimmermann

Cell site location information is no longer confined to crude approximations, but has become increasingly sophisticated and precise. The majority of Americans now carry their phones at

nearly all times, largely unaware that the devices are automatically creating a detailed and lasting record of their locations and movements. In the hands of law enforcement, these records have the potential to reveal a wide range of information about individuals' habits, activities, and associations.

Cellular carriers now routinely retain months and even years of CSLI data, on all of their users. And law enforcement increasingly requests large tranches of this information—making up many months—for their surveillance targets. The use of this information without adequate court supervision has the potential to profoundly unsettle legitimate expectations of privacy. Amici therefore urge the Court to treat this issue as the serious and growing challenge to individual privacy that it is, and to institute appropriate safeguards for CSLI use, including requiring law enforcement to obtain a warrant, subject to traditional Fourth Amendment standards, before obtaining or using it.

And in case you thought it was just left-leaning companies and individuals lining up:

US Justice Foundation, Gun Owners Foundation, Citizens United Foundation, Conservative Legal Defense fund et al

At the time of the ratification of the Fourth Amendment, it was generally understood that each person had a protected property interest not just in the things he owned, but first, as the Fourth Amendment text makes clear, in his "person." As made clear by giants like Blackstone and Locke, his right to his person encompassed his right to the labor of his body, his freedom of movement, and his right to communicate with and interact with others.

The government contends that defendants' transmission of CSLI was "voluntary," and its collection by cell phone providers was for the "business purposes" of their cellular providers. However, the government certainly cannot rely on supposed voluntary submission of data to a cell phone provider when it was the federal government that designed the very system of cell phone use that now exists.

Indeed, in order to communicate in today's modern world, defendants were forced onto government-controlled airwaves, on a government-approved cellular network, using government-mandated technology, transmitting government-required location data. Under such a system of pervasive control, the Orwellian tracking of Americans cannot be justified on a theory which presumes voluntary action and consent. Legalization of constitutional violations does not make them constitutional.

They even cite Ayn Rand later!

While this issue may seem like a no-brainer to some, the fact is there is a much-relied-upon precedent that benefits law enforcement and makes their job easier. Arguments will likely emerge over the practical costs of getting warrants for these common requests — i.e. criminals will get away while the paperwork is pending. There are no easy answers for that, considering the incredible amounts of red tape already involved in such things.

That said, if it's unconstitutional, it's unconstitutional — and that's what the Supreme Court is charged with determining. It may be that Congress and local government have to deal with the fallout.

Carpenter v. United States is on the court's October Term, but there are some serious cases on its plate (as there often are), including some important binding arbitration stuff and Trump v. Hawaii. So we'll see if there's time.