Needed: A Bill of Rights for the digital age

Patrick G. Eddington

June 26, 2018

Last week's Supreme Court split decision narrowly in favor of limited protections for your digital data and mine—the case of Carpenter v. United States—only underscored how far we have to go in making the Fourth Amendment meaningful in the Digital Age.

At issue in the case was whether police could continue to use cell-site location information (CSLI), generated by our cell phones literally every minute, without first obtaining a warrant. The Court's majority noted that CSLI gives "the Government near perfect surveillance and allow it to travel back in time to retrace a person's whereabouts, subject only to the five-year retention policies of most wireless carriers." For the Justices voting to overturn lower court rulings against the plaintiff, the real-time nature of CSLI and the aggregated historical movement tracking it offers were sensitive enough information to mandate the use of a probable cause-based warrant, per the Fourth Amendment's requirement.

But there's a key caveat to the decision: it leaves much of our digital data without similar protections. In his dissent, Justice Neil Gorsuch noted that prior Court rulings in the 1970s had opened the door to the kind of law enforcement abuses Carpenter complained of in his case. Gorsuch was referring to two cases: United States v. Miller and Smith v. Maryland.

In *Miller*, the court held that your bank records and mine, were not, in fact, our "papers and effects" (as defined in the Fourth Amendment), but instead "business records of the banks."

In *Smith*, the Court held that a device installed at a telephone service provider's office to track every call you or I make from our phones did not constitute a search under the Fourth Amendment, as we had no "expectation of privacy" when we "voluntarily conveyed numerical information to the phone company and "exposed" that information to its equipment in the normal course of business" and thus we "assumed the risk that the company would reveal the information to the police."

These two cases form the cornerstone of what's called in legal-speak the "third party doctrine"—Court-created carve outs of the Fourth Amendment that, for Gorsuch, constitute a direct attack on a core constitutional principle, as he noted in his dissent.

"What's left of the Fourth Amendment? Today we use the Internet to do most everything. Smartphones make it easy to keep a calendar, correspond with friends, make calls, conduct banking, and even watch the game. Countless Internet companies maintain records about us and, increasingly, *for* us. 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."

He's absolutely right. But Congress shouldn't wait for the next major court case challenging the "third party doctrine" in the hope that Gorsuch's position will finally sway his colleagues to kill this misguided legal notion.

The only way to guarantee the Fourth Amendment rights of Americans in the Internet Age is to make it explicitly clear in law that *any* digital data generated by our cellphones (whether for administrative (location tracking) or substantive (writing a blog post) purposes) is just that—our digital "papers and effects" that require a probable cause-based warrant for the government to seize and search. Congress has the power to do exactly that. Whether the *Carpenter* decision will be the motivation they need to do so remains to be seen.

Former House staffer and ex-CIA analyst Patrick Eddington is a policy analyst in civil liberties and national security at the Cato Institute.