September 17, 2013

Who Should be the 'Decider' on Keeping Our Secrets?

Stephen E Henderson, *University of Oklahoma College of Law*

Nothing Hid That Shall Not Be Known

by Stephen E. Henderson

The all-seeing Eye of Providence hovers omnisciently on the Great Seal of the United States, the familiar image replicated on the reverse side of the one-dollar bill. Yet in Tolkien's *The Lord of the Rings*, it is the malevolent eye of Sauron that peers everywhere, "piercing all shadows," seeking the One Ring that will finally allow him mastery over everyone and everything.

So perhaps it was not surprising that when a federal agency, spurred by the terrorist attacks of 9/11, adopted as its logo a hovering eye scanning the globe, accompanied by the motto "scientia est potentia" (knowledge is power), many were unsure of its intentions and Congress ultimately defunded the office. When J. Edgar Hoover gathered information for his FBI, he sometimes broke the law and sometimes skirted it. The terrorism surveillance initiatives of George W. Bush arguably did the same, and recently we have learned that much the same gathering continues under President Obama. We also recently learned that the US Postal Service records the exterior of every piece of mail it circulates, and that a partnership between AT&T and law enforcement (the "Hemisphere Project") adds four billion phone records a day to an enormous database dating back twenty-six years. Is this contemporary surveillance beneficent? Is it legal?

Just as it is difficult to pin down precisely what the NSA is collecting – perhaps, as security technologist Bruce Schneier has posited, we have to assume it gathers most everything – it is difficult to quickly explicate the many doctrines necessary to parse legality. If the gathering is meant to serve national security, meaning protecting against foreign powers and agents thereof, then the president has some inherent Article II authority, an authority that can be buttressed or weakened by the powers Article I provides Congress.

The resulting laws, including the Foreign Intelligence Surveillance Act, are no models of clarity. Thus we debate whether the infamous Section 215's permission to gather "any tangible things . . . [relevant to] an investigation . . . to protect against international terrorism" was meant to permit a dragnet sweep of all communications metadata, as is occurring. Or, as at least one legislative author has argued, was it meant to permit only targeted surveillance?

The primary source of constitutional restriction, the Fourth Amendment, protects the right of "the people" (itself a potentially complicated criterion) to be secure from unreasonable searches and seizures. Its restrictions are lesser when it comes to national security, including being markedly different at the international border, and for its interpretation we must look to the courts, perhaps including the Foreign Intelligence Surveillance Court that seems to resemble a court only in that it is populated by sitting Article III judges (it hears only from the government, and its proceedings and orders are secret).

Surely things get more straightforward when we leave the realm of national security and turn to domestic law enforcement? Yes and no. Here the Fourth Amendment law is much better explicated, but it is also confusing – some might say downright "confused" – and in flux.

For many years the Supreme Court has assured us that the Fourth Amendment protects "reasonable expectations of privacy," yet the Court has also created a "third party doctrine" that extinguishes constitutional protection for information provided to another. The cops want your bank records? No problem. If you wanted to restrict that information from the police, you shouldn't have shared it with the bank. So, the police can acquire that information with *no* constitutional restraint.

It doesn't take a privacy theorist to see that the Court has conflated secrecy with privacy or, if you prefer, with the explicitly constitutionally protected right to "security" in persons, papers, and effects. And in a digital world in which we leave fingerprints most everywhere we go – from the websites we visit, to the prescriptions we purchase, to the locations we travel, to the books we read and the television we watch – the third party doctrine potentially covers enormous ground.

In 2012, the Court began to come to grips with this reality when it unanimously restricted long-term GPS tracking of vehicles, an activity that some see as residing on the "easy" side of the third-party doctrine (your location is not provided to a single other person for a singular purpose, but instead is available to all comers). Although the Justices were far from unanimous in their reasoning, and that reasoning was far from complete, I have developed in my scholarship the view that the Court has been quietly chipping away at its own third-party limitation for the past quarter century.

Whatever the Supreme Court ultimately decides about the Fourth Amendment, our civil liberties are also protected by state constitutions (at least as against agents of that state), by state and federal legislation, and by administrative regulation. Increasing numbers of states are more generous in interpreting their constitutions, and legislatures in their legislation. But we face a fascinating conundrum. If private parties, and then through them the State, can know *everything*, is that a good thing akin to the Eye of Providence, or more akin to that of Sauron?

Ubiquitous computing, also known as the "Internet of Things," is approaching reality. Soon your own clothes may be "phoning home" to report on you (and you thought it was acceptable to pair those shoes and slacks). Surveillance drones hovering at 20,000 feet and equipped with gigapixel cameras can watch overhead all day; cameras you install in your home and access online can watch inside; and body cameras will record everything we do (only one limited manifestation being the new Google Glass). Big Data companies from Palantir to Facebook to IBM push the science of analytics to make sense of the now overwhelming amounts of information that are gathered.

A friend recently passed along a science fiction story written in 1948 (Lewis Padgett's *Private Eye*). In this imagined world, everything – from the walls to the sand on the seashore – has been found to record what transpires before it. Obviously in a sense privacy as we know it would be dead, but not entirely, because the society passes laws that permit accessing this data only upon good cause, and then only about a particular individual or issue of interest.

It seems we must soon confront this same question. As ubiquitous, latency-free storage becomes possible, should we give up our traditional restrictions upon acquiring information, retaining everything, and rely entirely upon ex-post use and dissemination controls? Or, on

account of the inevitable abuse that would permit, and given the chilling effects that will have, is it sometimes better that we know less even though some attacks will not be prevented and some guilt will go unpunished? And for what information is known, should it be held only privately, or also by the government? Is that even a difference that matters if the two work so closely together that the government pays to embed private employees in its ranks, as with the Hemisphere Project?

The Fourth Amendment long ago struck a perhaps designedly ambiguous balance of "reasonableness." The George W. Bush and Obama Administrations have, largely in secret, made the decision for telephone metadata, international communications, and perhaps for much else besides. Have they chosen rightly? And in a democracy, should they be – to paraphrase "W" – the decider?

Stephen Henderson is a Professor of Law at The University of Oklahoma.