Published by *Just Security* on February 3, 2014.

Quantum Mechanics, Big Data and the Right of Privacy

--By Charles A. Blanchard, Arnold & Porter LLP

If it has done nothing else, the exposure of the NSA metadata collection program has caused both legal commentators and courts to rethink the doctrines that have long governed the law of search and seizure and privacy. Is "reasonable expectation of privacy" a viable concept given our networked lives? Does the holding of *Smith v. Maryland* that there is no reasonable expectation of privacy for information given to a third party offer too little protection from mass surveillance given modern technology?

These questions are becoming even more important as both governments and private companies find the analytic tools of "big data" increasingly useful. These tools allow us to find the proverbial needle in a haystack–and can be used to save lives–but they only work if we allow collection of the haystack in the first place. How do we think about privacy of big data? Is there a way that we can take advantage of the potential power of "big data" without sacrificing our privacy?

As strange as it may seem, quantum mechanics might help us illuminate the best approach to restrictions on surveillance. Just as quantum mechanics teaches that matter has no certainty in position, spin, momentum and other properties until we actually seek to measure or observe matter, the privacy interests at the core of the Fourth Amendment are only implicated when officials search the data.

In 1979, the Supreme Court decided *Smith v. Maryland,* which held that a defendant had no reasonable expectation of privacy in the numbers dialed from his phone because he voluntarily transmitted them to the telephone company. The Court concluded that giving such information to a third party eliminated any reasonable expectation of privacy. This was a pretty extraordinary holding because it meant that Fourth Amendment protections did not even apply to law enforcement requests for telephone numbers called. And, it was this case that the FISA Court relied on–heavily–in upholding the NSA metadata collection.

Even before the NSA metadata program was disclosed, Justice Sotomayor's concurrence in *United States v. Jones* made a strong case that *Smith v. Maryland* was simply not sufficient given modern technology. As, she said "[t]his approach is 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. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers."

So given this reality, how do we approach government compelled collection and use of metadata and other "big data?"

Here is where quantum mechanics comes into play. According to quantum mechanics, matter such as an electron or photon is described by a probability wave function and does not have a precise physical state. This does not mean merely that we don't know the precise state of a proton or electron–it means that the proton or electron truly has no precise state at all. But when we attempt to measure the state of a proton or electron, something almost magical occurs–the probability wave function collapses into a measurable physical state.

What does this have to do with privacy? Much of the metadata collected remains as nothing more than a collection of ones and zeros never examined by a human being. In this form, nothing about our lives is communicated to anyone. We remain anonymous. Our activities are, for all practical purposes, unknown. This is just like an electron in its uncertain waveform state. This all changes, however, when a government analyst does a search of the collected data. The ones and zeros become intelligible and meaningful. Our activities, and perhaps even our identity, are revealed–often with intrusive detail. The potential for government abuse and intrusion becomes very real as well. Just as a quantum wave function collapses into certainty by measurement, government intrusions into privacy become real and concrete when the data is searched.

What does this mean for the *Smith* third party rule? It needs to be revamped to separate our analysis of collection and use. *Smith* does not distinguish compelled collection from use. Under *Smith*, even the use of the data (such as a search by an analyst) does not implicate the Fourth Amendment because we are deemed never to have had a reasonable expectation of privacy in the data in the first place. Once collected, there are no restrictions on the use of the data. As Justice Sotomayor observes, this effectively eliminates any privacy rights we have on the Internet. We need to apply a higher standard on each ***use*** of any government compelled data collected to offer a more realistic protection of privacy and to prevent government abuse. In many cases, this should mean the normal Fourth Amendment reasonable search and warrant requirements on searches of the collected data.

But it also means that mere collection of digital data itself does not necessarily implicate privacy interests absent any search or use of the data. For purposes of mere collection the *Smith* holding can still stand. For prudential reasons, we obviously may want to apply significant oversight and control over the compelled collection and storage of metadata and other "big data," with special protection for data that could lead to special harm such as medical or financial data, or data about the exercise of constitutional rights. As a check on government misuse, we might even want to keep the data out of the control of the government until judicial approval is obtained. Our true privacy interests are implicated by the use of the compelled collected data, however, and not by the collection itself.

Charles A. Blanchard is a partner with Arnold & Porter. He served as General Counsel of the Air Force from 2009 and as General Counsel of the Army from 1999-2001. Follow him on Twitter @FmrAirForceGC.