U.S. Court Rules NSA Bulk Data Collection Unconstitutional

*Rutgers University Law Professor and LSE Visiting Fellow **Ellen Goodman** explains the landmark decision against NSA surveillance recently made in the US, pointing out the importance of scale and changes to the constitutional meaning of communications.*

On 16 December U.S. federal district court Judge Richard Leon (Washington D.C.) held in a 68-page opinion that the NSA's bulk collection of mobile phone call "metadata" was an unconstitutional violation of privacy. The effect of the decision is stayed pending appeal, but the court's reasoning is instructive.

Essentially, the judge found that:

1) our current use of communications devices fundamentally changes the constitutional meaning of call logs, upending old assumptions about what information this data reveals and the strength of individual liberty interests in keeping the government out of it, and

2) scale and efficiencies matter –data collection practices that are permissible when they are expensive for the government to deploy and small in scale might not be permissible when the practices are cheap and deployed on a massive scale.

This reasoning, if sustained, has big implications for government use of big data and conceptions of liberty in the digital world.

The government's argument was that Americans have no expectation of privacy in the numbers they call or the duration of those calls. The controlling precedent, according to the government, is a 1979 Supreme Court case, Smith v. Maryland. This was a case in which police were investigating a robbery victim's reports that she had received threatening calls from the alleged robber (Smith). Using a warrantless pen register, the police traced such a call to Smith's home phone. The Supreme Court ruled that Smith had no expectation of privacy in the phone call data – as opposed to the phone call content – because he had voluntarily released that data to the phone company.

The NSA's program is very different from this analog police trace, Judge Leon found. In reaching this decision, he relied on a 2012 Supreme Court case, United States v. Jones. There, the question was whether government use of a GPS tracking device to monitor an individual's movements over a long period of time violated the target's privacy. A majority of five justices said that this kind of surveillance was unlike the short-term monitoring of a suspect's movements that had previously been found acceptable. They reasoned that the increased scale of the surveillance and information-yield make a difference. What the government can get from long-term and comprehensive monitoring dwarfs the product of the limited monitoring of old.

So too, with the bulk-data collection, Judge Leon found four differences from the pen-register case:

1. **Nature of data collection.** Whereas Smith involved a short-term, forward-looking, and non-retentive data collection, the NSA's program is long-term, backward looking, and retentive; it retains data for five years and is able to develop detailed historical profiles.

2. **Role of communications companies.** Whereas Smith involved a one-time (or at least relatively rare) provision of information by the phone company to the police, the NSA program involves ongoing cooperation by the companies who are essentially enlisted into "a joint intelligence- gathering operation with the Government."

3. **Scale of data collection.** Individualized data collection of the old kind was expensive and burdensome. Bulk collection of metadata is cheap. The implication is that the cost-benefit analysis that might once have served to check the government's appetite for surveillance works out differently now. In the absence of serious economic constraint on surveillance, the constitutional constraint may have to be greater.

4. **Knowledge produced by data.** Mobile phone ubiquity and constant usage has exploded the quantity of metadata and, more importantly, the information it yields about people's lives. The court correlates this increased yield to rising expectations of privacy, even though the data itself is "released" to the communications carriers.

Not all these distinctions are strong or likely to hold up on appeal. It's not clear, for example, why the extent of cooperation by the phone companies should matter to the individual's expectation of privacy. The court's most persuasive rationale for treating the NSA's bulk data collection differently from more discrete collections of data is the information yield.

While individuals may not have an expectation of privacy with respect to discrete pieces of data collected by third parties, their interests change with scale. Substantial quantities of data points gathered over a long period of time render mere metadata much more informative. The difficulty with this reasoning is that it makes the leap from the information yield of the data to individual expectations of privacy – a leap that a majority of justices seem sympathetic to, but that the Supreme Court has not endorsed.

Much will depend on the case that the government can make about the privacy/security balance and the utility of the bulk data collection. Members of Congress have praised the decision and urged that the Supreme Court take up the matter, which it is all but certain to do.

This blog post gives the views of the author, and does not represent the position of the LSE Media Policy Project blog, nor of the London School of Economics.

December 18th, 2013 | Guest Blog, Internet Governance, Privacy | 0 Comments