Court ruling against NSA practice could reverberate far beyond phone spying

The federal court decision Thursday that found it illegal for the National Security Agency to collect massive amounts of phone data may have broader implications when it comes to privacy in the Digital Age.

By Joe Uchill

May 8, 2015

The federal court ruling Thursday that found it illegal for National Security Agency to collect massive amounts of information on Americans' phone calls could impact more than just the spy agency's practices.

The Second Circuit Court of Appeals decision in the American Civil Liberties Union v. Clapper case could affect other government surveillance programs, impede the government's ability to execute warrants to access data stored on overseas servers, and even change how electronic data is treated in future court rulings, according to legal experts.

“There are privacy implications that go beyond this NSA program,” says Elizabeth Goitein, the codirector of the liberty and national security program at New York University’s Brennan Center for Justice.

The federal case centered on the Patriot Act's Section 215, which the government has used as a justification for the NSA's practice of collecting phone metadata. That program was revealed by ex-NSA contractor Edward Snowden and, since then, supporters of the surveillance practice have pointed to Section 215 as its legal justification.

Section 215 does allow for the collection of “relevant” data for an authorized investigation. In the federal case, attorneys for the US argued that any data – even data that had no relationship to any investigation – was relevant, because the mass of data might be relevant to future investigations.

Circuit Judge Gerard Lynch disagreed. "Relevance does not exist in the abstract; something is ‘relevant’ or not in relation to a particular subject," wrote Judge Lynch.

The ruling comes as Congress is considering whether to reauthorize the parts of the Patriot Act, including Section 215, because they are set to expire on June 1. The court decision will certainly put new pressure on lawmakers who support the surveillance program, and give more fuel to those who oppose it and seek to reform the NSA's bulk collection programs.

But relevance arguments similar to the one the court denounced have also been used by the US government to justify other data collection or surveillance efforts. This ruling will likely impact those programs – and others that involve the mass collection of electronic records in the US or abroad.

"The government has used this argument about relevance in two other surveillance programs that are no longer in operation. More than likely, they would be interested in using the argument again for future programs," says Ms. Goitein.

For instance, one programs that used a similar argument was a Drug Enforcement Administration operation to collect international telephone metadata. A federal court in California ruled in April that the defunct DEA program violated the Constitution.

In addition to the question of relevance addressed in the court's Section 215 ruling, the Second Circuit also found that a government search of data begins when it is first collected, not at the moment when computer analysis of that data triggers any kind of investigation.

This definition of search could also have bearing on other ongoing cases that involve the government's access to electronic data, says Goitein.

One major case involves Microsoft. The tech giant has been fighting a government warrant that seeks to gain access to data stored in servers located in Ireland. Microsoft contends the data is held beyond the reach of the US government.

But the US argues it has the right to search those servers because it could execute the warrant from within the US. Thursday's ruling could add weight to Microsoft's case since the court ruled that a "search" takes place when the data is collected, not when it's examined.

Indeed, data may begin being treated more like real property as a result of the Section 215 decision, says Jim Harper, a senior fellow at the CATO Institute and a founding member of the Department of Homeland Security’s Data Privacy and Integrity Advisory Committee.

“The court ruled very clearly on standing, data had to be treated as something to be seized,” says Mr. Harper. The court went as far as italicizing seizure when describing its importance in standing. “For courts to grapple with the data issue they have to come to that conclusion – that data is property.”

Information is currently not treated as property in terms of search and seizure. Instead, courts issue warrants with the expectation that information will be kept private. But that expectation of privacy disappears when data is viewed by a third party.

In United States v. Jones, a case about law enforcement placing a GPS tracker on a suspect's car, Justice Sonia Sotomayor bemoaned that the expectation of privacy “is ill-suited to the Digital Age, in which people reveal a great deal of information about themselves to third parties" – including to Internet service providers and cellphone companies.

But Harper says that viewing information as property solves Justice Sotomayor’s problem. If metadata is property, it becomes easy to determine its Fourth Amendment standing.

“The main point of the Second Circuit rule was about the NSA collections, but look at how they got to that decision,” he says. “It could have a greater impact.”