Written by **Thomas R. Eddlem** on December 27, 2013

N.Y. Judge: NSA Spying "Imperils Civil Liberties of Every Citizen" but "Legal"

Southern District of New York Judge William Pauley III declared in a December 27 decision that the NSA surveillance program — which draws in every American's telephone records without a warrant or probable cause — was "legal" even though it "imperils the civil liberties of every citizen." The decision contrasts sharply with a decision two weeks ago by Washington, D.C. District Court Judge Richard Leon that termed the warrantless surveillance program unconstitutional and "almost Orwellian."

Almost Orwellian was no problem for Pauley, who found that the Constitution should not get in the way of programs the government claims have worked: "The question for this Court is whether the Government's bulk telephony metadata program is lawful. This Court finds it is."

Pauley dismissed the lawsuit by the ACLU despite acknowledging that "This blunt tool works because it collects everything. Such a program, if unchecked, imperils the civil liberties of every citizen."

Metadata is the record created by a telephone call, and includes the number calling and the number called, as well as the time and duration of the call. The NSA also has other programs to collect Internet traffic and other data on Americans, but these other programs were not the subject of the lawsuit dismissed by Pauley.

Pauley claimed, however, that "Bulk telephony metadata collection is subject to extensive oversight by all three branches of government. It is monitored by the Department of Justice, the Intelligence Community, the FISC [Foreign Intelligence Surveillance Court], and Congress."

Pauley's claim is not backed up by the facts, nor even by the text of his own 54-page decision. The public record is devoid of any serious restrictions on NSA created by the intelligence community or the Justice Department. And the FISC has turned out to be an NSA lapdog, not a watchdog. The *Wall Street Journal* reported back on June 9 that "From 1979 through 2012, the court overseeing the Foreign Intelligence Surveillance Act has rejected only 11 of the more than 33,900 surveillance applications by the government, according to annual Justice Department reports to Congress."

Indeed, Pauley's decision — despite touting "extensive oversight" from FISA courts — acknowledged "there is no way for the Government to know which particle of telephony metadata will lead to useful counterterrorism information. When that is the case, courts routinely authorize large-scale collections of information, even if most of it will not directly bear on the investigation."

As for Congress' surveillance of the NSA, most members didn't even know about the program until Edward Snowden revealed it to the public. Rep. Justin Amash (R-Mich.) noted that NSA briefings of

Congress amounted to "a totally ridiculous game of twenty questions."

The court decision read more like an op-ed by NSA chief Keith Alexander than a neutral court ruling, as Pauley derided "judicial-Monday-morning-quarterbacking" by the Leon court. Throughout the wordy 54-page decision, Pauley never articulated any objective restriction on a search that would be a violation of the Fourth Amendment. Not, at least, an argument on the Fourth Amendment that would be even a "substantial" burden on the government. Pauley noted that "To obtain a section 215 order [under the Patriot Act], the Government must show (1) 'reasonable grounds to believe the tangible things south are relevant to an authorized investigation.'" But the "reasonable" standard is one defined by the U.S. Constitution's Fourth Amendment. Pauley argued that "Under section 215, the Government's burden is not substantial." But the Fourth Amendment explicitly defines a "reasonable" search as one with a warrant supported by an oath, probable cause and particularity in describing what will be found and where it will be found.

Pauley claimed in his decision that "The collection of breathtaking amounts of information unprotected by the Fourth Amendment does not transform that sweep into a Fourth Amendment search." Of course, all searches are subject to the Fourth Amendment; the amendment makes no exceptions for non-Fourth Amendment searches. The text of the Fourth Amendment reads:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The New York court's decision revealed how courts can "interpret" a constitutional amendment out of existence. Pauley openly acknowledged in his decision that the NSA program does not comport with the Fourth Amendment's "probable cause" requirement, writing that "Any individual call record alone is unlikely to lead to matter that may pertain to a terrorism investigation." He also acknowledged that the NSA-backed surveillance did not comport with the warrant requirement through National Security Letters issued by the FBI: "An NSL does not require judicial approval."

Pauley based his constitutionality ruling on the claim in his decision that "an individual has no legitimate expectation of privacy in information provided to third parties" and that "when a person voluntarily conveys information to a third party, he forfeits his right to privacy in that information." Of course, while his court claimed that a person has no right to claim privacy in any third party records voluntarily created, the Federal Trade Commission was busy suing businesses such as Google for violating this same non-existent privacy violation. Google paid a $22.5 million fine in 2012 for putting "cookies" on browsers that used its websites after being taken to court by the Federal Trade Commission. So if there's no legitimate right to privacy, why did the Obama administration — the same branch of the federal government that claimed there's no reasonable expectation of privacy in the NSA lawsuit — sue Google?

Moreover, Pauley took pains to stress that the NSA keeps the data private, writing that "The NSA store the metadata in secure networks and access is limited to authorized personnel." If there's no reasonable expectation of privacy, why all the secrecy and restricted access?

Pauley's claim that the information is "secure" is false on its face. Edward Snowden's release of the information alone is proof that the information is not secure, and Pauley acknowledged that the lawsuit was possible only because of Snowden's revelations. Snowden was a 27-year-old contractor for Booz-

Allen-Hamilton — not even an NSA employee — who had access to this sensitive information. And the NSA has admitted a dozen other instances of abuse of that "metadata" information, in some instances where NSA employees were using the data to spy on their wives and girlfriends.

This, of course, puts the lie to Pauley's claim that "the Government does not know who *any* of the telephone numbers belong to." [Emphasis in original.] Of course, if they don't know to whom any of the numbers belong, how did NSA employees know enough to zoom in on their girlfriends and wives?

The revelation that NSA employees were using the surveillance program as a crutch for their failing romantic relationships also puts the lie to Pauley's claim in his decision that "There is no evidence that the Government has used any of the bulk telephony metadata it collected for any purpose other than investigating and disrupting terrorist attacks."

The December 27 decision did put the USA Patriot Act in its proper light, however. Pauley noted that one provision of the Patriot Act was "eliminating the restrictions on the types of businesses that can be served with such orders [broad demands for private information without a search warrant] and the requirement that the target be a foreign power or agent." In other words, the Patriot Act was written to allow the government to target Americans — for the first time — for surveillance. "The ACLU argues that the category at issue — all telephony metadata — is too broad and contains too much irrelevant information. That argument has no traction here. Because without all the data points, the Government cannot be certain it connected the pertinent ones." Indeed, Pauley stressed that "the Government invoked this authority to collect virtually all call detail records or 'telephony metadata.'"

One can paraphrase Pauley's decision as essentially one where "one nation under surveillance" is an acceptable way of life, and where the Fourth Amendment is a relic of a bygone era without any "substantial" impact on the federal government.