IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF IDAHO

ANNA J. SMITH Plaintiff, v. BARACK OBAMA, President of the United States, et al., Defendants.	Case No. 2:13-CV-257-BLW **MEMORANDUM DECISION**

INTRODUCTION

The Court has before it plaintiff Smith's motion for injunctive relief and defendants' motion to dismiss. The Court heard oral argument on May 14, 2014, and took the motions under advisement. For the reasons expressed below, the Court will grant the defendants' motion to dismiss and deny Smith's motion for injunctive relief.

BACKGROUND

The Fourth Amendment protects the right of privacy by forbidding unreasonable searches and seizures. With few exceptions, a citizen cannot be searched in violation of her reasonable expectation of privacy unless a judge has found there is probable cause to believe that she is committing a crime. This Fourth Amendment protection is violated here, Smith alleges, because the National Security Administration (NSA) is searching her telephone records without showing first that there is probable cause to believe she is engaged in criminal behavior. She asks the Court to enjoin the NSA from collecting and analyzing her telephone data.

For more than seven years, the NSA has been collecting and analyzing the telephone records of Americans to detect terrorist threats. While the agency does not listen to conversations, or identify the callers' names and addresses, it does collect the telephone numbers of all parties to a call, along with the duration and time of that call, and stores this data for five years.

The NSA's collection and analysis protocols must be periodically approved by the Foreign Intelligence Surveillance Court (FISC). The FISC prohibits the NSA from accessing the stored telephone data for any purpose other than counterterrorism or technical maintenance of the system. *See Shea Declaration (Dkt. No. 15-2)* at ¶ 31.

The NSA uses its vast trove of data to identify the telephone numbers of calls that terrorists make and receive. Before the NSA can access its telephone data, the FISC-approved protocols require the agency to first make an internal finding – authorized by one of twenty-two designated NSA officials – that a particular telephone number is associated with a terrorist organization. *Id.* at ¶ 32.

Once the NSA makes its internal determination, it may run a query through its data bank to collect (1) the telephone data of persons who made calls to – or received calls from – the suspected terrorist, and (2) the telephone data of persons who made calls to – or received calls from – the telephone numbers for any person who had direct telephone contact with the suspected terrorist. *Id.* at ¶ 23. In prior years, the scope of the query extended to a third level but "the NSA has taken immediate steps to implement restrictions [imposed by the President] limiting its review of queries to two [levels] only

and the Government is now working with the FISC to incorporate this restriction into the FISC's orders." *Id*.

Smith alleges that her own telephone data has been swept up into the NSA's broad net in violation of her Fourth Amendment rights.[1] She asks the Court to enjoin the agency from collecting and using this telephone data from her calls.[2]

ANALYSIS

The Fourth Amendment is concerned with surveillance that (1) involves a "trepassory intrusion on property" or (2) "violates a subjective expectation of privacy that society recognizes as reasonable." *See U.S. v. Jones*, 132 S.Ct. 945, 954-55 (Sotomayor, J., concurring). It is the latter interest that Smith urges here. She claims that the NSA's collection efforts violate her expectation of privacy in her telephone records.

Smith has no expectation of privacy in the telephone numbers that she dials. *See Smith v Maryland*, 442 U.S. 735 (1979). A person using the telephone "voluntarily convey[s] numerical information to the telephone company" and "assume[s] the risk that the company [will] reveal to police the numbers he dialed." *Id.* at 744.

But the data collected by the NSA goes beyond the telephone numbers that Smith dials, and reaches into her personal information. For example, the NSA's collection of

[1] Smith originally alleged additional claims but has conceded that they should be dismissed, leaving only the Fourth Amendment claim for resolution.

[2] The Court finds that Smith – a Verizon customer – has standing to bring this action. *See Klayman v. Obama*, 957 F.Supp.2d 1, 26-28 (D.D.C.2013) (granting standing to individual plaintiffs to challenge NSA collection of their telephone records from Verizon after finding "strong evidence" that NSA has collected Verizon metadata for the last seven years and run queries that necessarily analyzed that data).

the time and duration of phone calls is revealing: Would most citizens want to keep private the fact that they called someone at one in the morning and talked for an hour or two?

And what about location? Would most phone users expect to keep private (1) their location at any moment and (2) their travel path over time? The NSA collects "trunk identifier" data, *see Shea Declaration, supra* at ¶ 15, that shows the location where a cell-phone call enters the "trunk" system to be relayed eventually to the number being called. *See* Leslie Groll, *What Kind of Phone Data Can the NSA Collect Exactly?*, FOREIGN POLICY (June 6, 2013).[3] While this would not pinpoint a phone user's precise location, it would narrow it down considerably. *Id.*[4]; *see also State v. Earls*, 70 A.3d 630, 637 (N.J.Sup.Ct. 2013) (holding that New Jersey's constitution requires police to obtain warrant before collecting cell phone location data and noting that carriers have data that "can locate cell-phone users within buildings, and even within individual floors and rooms within buildings"). Moreover, the data also includes "comprehensive communications routing information." *See Shea Declaration, supra* at ¶ 15. While this phrase is ambiguous, it may mean that for a single call, all the trunk identifiers are collected by the NSA, allowing the agency to track "how a cell phone user moves from

[3] Available at http://blog.foreignpolicy.com/posts/2013/06/06/what_kind_of_phone_data_can_the_nsa_collect_exactly

[4] Trunk identifier data may be used to "locate a phone within approximately a square kilometer." Patrick Di Justo, *What the N.S.A. Wants to Know About Your Calls*, NEW YORKER (June 7, 2013), http:// www.newyorker.com/online/blogs/elements/2013/06/what-the-nsa-wants-to-know-about-your-phone-calls.html.

one cell phone tower to another while traveling." FOREIGN POLICY, *supra.* The speed with which the phone moves from tower to tower could indicate, for example, whether the device is being used in a car or while walking down the street.

Compare these intrusions to those faced in *Smith:* There, the Baltimore police collected the telephone numbers dialed by a suspected robber for about two days. This simple comparison reveals a looming gulf between *Smith* and this case. But the Ninth Circuit has bridged some of that chasm. In *United States v. Reed,* 575 F.3d 900 (9th Cir. 2009), the Circuit held that "there is no Fourth Amendment expectation of privacy" in data that includes the number dialed along with the length and time of the call. *Id.* at 914. The Circuit has also applied *Smith* in holding that e-mail and internet users have no expectation of privacy in the "to/from addresses of e-mail messages, the IP addresses of websites visited and the total amount of data transmitted to or from an account." *U.S. v. Forrester,* 512 F.3d 500, 510 (9th Cir. 2008). To the extent that an individual's telephone data collected by a cell-phone provider is no different than an individual's power consumption records collected by an electric utility, the Circuit has held that utility customers lack a reasonable expectation of privacy in such business records. *U.S. v. Golden Valley Elec. Ass'n,* 689 F.3d 1108, 1116 (9th Cir.2012).

Although the Ninth Circuit has not resolved the precise issue faced here, other courts have done so: Two of these decisions apply *Smith* to find that the NSA is not violating the Fourth Amendment. *See A.C.L.U. v Clapper,* 959 F.Supp. 2d 724 (S.D.N.Y. 2013); *U.S. v. Moalin,* 2013 WL 6079518 (S.D.Cal. 2013).

But these cases do not address a subject lurking in the shadows here: The possibility that the NSA is tracking the location of calls using the trunk identifier data discussed above. In *Jones*, five Justices wrote that the government surveillance of one's public movements for 28 days using a GPS device violated a reasonable expectation of privacy and constituted a Fourth Amendment search. *See also,* Case Comment, *Fourth Amendment – Warrantless Searches,* 127 Harv.L.Rev. 2164 (2014) (concluding that "[b]ecause the disclosure of [cell-site location information] is not necessarily voluntary, individuals still may hold an expectation of privacy in their cell-site data even under *Smith*").

The NSA denies that it is tracking location. Teresa Shea, the NSA's Director of the Signals Intelligence Directorate represents to the Court that "[t]he metadata collected by the Government pursuant to these [FISC] orders also does not include cell site locational information." *Shea Declaration, supra* at ¶ 15. A similar representation was made by the NSA's General Counsel, Robert Litt when he stated that "I want to make perfectly clear we do not collect cellphone location information under this program, either GPS information or cell site tower information."[5] Finally, the FISC orders submitted to the Court expressly prohibit the NSA from collecting any addresses

[5] *See Klayman*, 957 F.Supp.2d at 36 n. 57 (citing Transcript of June 25, 2013 Newseum Special Program: NSA Surveillance Leaks: Facts and Fiction, Remarks of Robert Litt, Gen. Counsel, Office of Dir. of Nat'l Intelligence, available at http://www.dni.gov/index.php/newsroom/speeches–and–interviews/195–speeches–interviews–2013/887–transcript–newseum–special–program–nsa–surveillance–leaks–facts–and-fiction).

associated with the telephone numbers it collects, apparently precluding the collection and analysis of location data. *See Order (Dkt. No. 15-6)* at pg. 3.

Smith's briefing and argument were not extensive on this issue. While there is speculation that the NSA is tracking location, there is no evidence of that, and the agency denies it. Under these circumstances, the Court will not assume that the NSA's privacy intrusions include location tracking.

Because *Jones* does not apply, the weight of the authority favors the NSA. The Supreme Court's decision in *Smith,* supplemented by the Circuit's decisions in *Reed, Forrester,* and *Golden Valley,* and the two District Court decisions on point, *Clapper* and *Moalin,* support a finding that there is no Fourth Amendment violation here.

The contrary view is stated by *Klayman v. Obama,* 957 F.Supp.2d 1 (D.D.C.2013), a thoughtful and well-written decision by Judge Richard Leon. He distinguished *Smith* by finding that the scope and duration of the NSA's collection is far beyond the individual pen register at issue in *Smith.* Of critical importance to Judge Leon was that *Smith* could never have anticipated the ubiquity of cell-phones and the fact that "people in 2013 have an entirely different relationship with phones than they did thirty-four years ago." *Id.* at 36. As he eloquently observes, "[r]ecords that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic—a vibrant and constantly updating picture of the person's life." Ultimately, he held that the plaintiffs had a likelihood of success on their Fourth Amendment claim, and he enjoined the NSA from collecting their telephone records, although he stayed his decision pending appeal.

Judge Leon's decision should serve as a template for a Supreme Court opinion. And it might yet. Justice Sotomayor is inclined to reconsider *Smith*, finding it "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." *See U.S. v. Jones*, 132 U.S. 945, 957 (2012) (Sotomayor, J., concurring). The Fourth Amendment, in her view, should not "treat secrecy as a prerequisite for privacy." *Id.*

But *Smith* was not overruled, and it continues – along with the Circuit decisions discussed above – to bind this Court. This authority constrains the Court from joining *Klayman.* Accordingly, the Court will grant the defendants' motion to dismiss and deny Smith's motion for injunctive relief. The Court will issue a separate Judgment as required by Rule 58(a).

DATED: June 3, 2014

B. Lynn Winmill
Chief Judge
United States District Court