UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION FOUNDATION; NEW YORK CIVIL LIBERTIES UNION; and NEW YORK CIVIL LIBERTIES UNION FOUNDATION, Plaintiffs, v. JAMES R. CLAPPER, in his official capacity as Director of National Intelligence; KEITH B. ALEXANDER, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service; CHARLES T. HAGEL, in his official capacity as Secretary of Defense; ERIC H. HOLDER, in his official capacity as Attorney General of the United States; and ROBERT S. MUELLER III, in his official capacity as Director of the Federal Bureau of Investigation, Defendants.	**SUPPLEMENTAL DECLARATION OF PROFESSOR EDWARD W. FELTEN** Case No. 13-cv-03994 (WHP) **ECF CASE**

SUPPLEMENTAL DECLARATION OF PROFESSOR EDWARD W. FELTEN

I, Edward W. Felten, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the following is true and correct:

1. Counsel for Plaintiffs in this lawsuit have asked me to submit a supplemental declaration explaining my views regarding four technological claims made by the government in its opposition to Plaintiffs' motion for a preliminary injunction:

   a. that the government does not obtain subscriber names under the mass call-tracking program, *see, e.g.*, Gov't PI Opp. 12;

   b. that so-called "three-hop analysis" of a suspect's phone number "cannot be as effectively performed" without first building a database of everyone's call records, *see, e.g.*, Gov't PI Opp. 4;

c. that telephony metadata is unique in its "standardized and inter-connected" nature, *see, e.g.*, Gov't PI Opp. 21; and

d. that it would take the government "approximately six months" to develop a method of quarantining Plaintiffs' call records if a preliminary injunction were granted, *see* Gov't PI Opp. 40.

2. Below, I address those four claims.

It is easy to correlate telephone numbers with subscriber names.

3. The government repeatedly emphasizes in its motion that, under the mass call-tracking program, it does not obtain the subscriber names associated with Americans' telephone numbers. This may be true, but it is of little significance. As I explained in my first declaration, Felten Decl. ¶ 19 & n.14, it would be trivial for the government to obtain a subscriber's name once it has that subscriber's phone number. This is so because phone numbers are unique identifiers. Like social security numbers or individual taxpayer identification numbers, phone numbers are unique to their owners.

4. It is extraordinarily easy to correlate a phone number with its unique owner. Many phone numbers are *publicly* correlated with their owners and can therefore be associated with specific persons by consulting entirely public sources. For example, many free or low-cost Internet services allow users to perform "reverse-lookup searches" to determine the owner of a particular phone number. *See, e.g.*, http://www.whitepages.com; http://www.peoplefinders.com/reverse-phone-directory. Of course, physical phone directories remain in wide circulation and have been digitized to facilitate reverse-lookup searches.

5. The government also has an array of legal authorities at its disposal to discover the subscriber names of particular phone numbers, even if those correlations are not otherwise publicly available. For example, the government may issue demands to communication service

providers for subscriber information—including subscriber names and addresses—relevant to terrorism investigations. *See* Felten Decl. ¶ 19 n.14.

Three-hop analysis can be performed without a database of all call records.

6. The government states that it could not perform three-hop analysis on a suspect's phone number without first building a database of *everyone's* call records. *See* Gov't PI Opp. 4. This is technologically incorrect. There are a number of ways in which the government could perform three-hop analysis without first building its own database of every American's call records.

7. For example, the government could obtain a single court order directing all (or perhaps even just the major) telephone companies to provide to the government the call records of everyone within three hops of a suspect's phone number. Using a straightforward algorithm (which I could describe at greater length if necessary), this order could be implemented using at most two queries to each telephone provider. Moreover, this process could easily be automated to make it virtually instantaneous. Each of the major telephone companies now subject to an order similar to the one revealed in June could create a simple electronic interface—known in the computer-programming profession as an Application Programming Interface, or API—that would be invoked by a government computer system to automate the collection of the data needed for a three-hop analysis of a specific target's phone number. The interfaces, working together to implement the algorithm referred to above, could perform the government's three-hop analysis essentially instantaneously—in a matter of seconds or less. At least one of the major telecommunications companies has already built part of such a system, providing the government with a "community of interest" search capability, which is a form of the social-graph analysis used in the mass call-tracking program. *See* Dep't of Justice, Office of the Inspector

Gen., *A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records* 56–64 (2010), http://www.justice.gov/oig/special/s1001r.pdf; Eric Lichtblau, *F.B.I. Data Mining Reached Beyond Initial Targets*, N.Y. Times, Sept. 9, 2007, http://nyti.ms/g34M.

8. I have reviewed the declarations submitted by Teresa Shea and Robert Holley in support of the government's claim that the collection of all Americans' call records is necessary. Nothing in their explanation of the supposed necessity of the program alters my conclusion that three-hop analysis could be performed quickly and efficiently *without* first creating a database of the scope maintained by the government. For example, Ms. Shea suggests that the mass call-tracking program would have allowed the government to learn that a 9/11 hijacker (Khalid al-Mihdhar) was in the United States when he communicated with an al Qaeda safe house in Yemen. Shea Decl. ¶ 11. There is absolutely no need for a database of every American's call records to perform this sort of one-hop analysis. In al-Mihdar's case, the government could easily have obtained from the telephone companies (using any number of legal authorities) the call records of any American in communication with the al Qaeda safehouse. The same is true of the example provided by Mr. Holley of Najibullah Zazi. *See* Holley Decl. ¶ 26. Mr. Holley states that the NSA received Zazi's telephone number from the FBI and discovered that he was in contact with Adis Medunjanin. Again, this simple connection could have been discovered directly from the telephone companies without the need for a government database of all call records. As I explained above, though, even if these cases involved more complex connections with two or three degrees of separation, there still would be no need for the mass call-tracking program to allow the government to discover the connections.

Telephony metadata is not unique.

9. The government argues that telephony metadata is unique in that it is "standardized and inter-connected," and that these characteristics are "not common to most other types of records." Gov't PI Opp. 21. This suggestion is misleading.

10. As I explained in my first declaration, Felten Decl. ¶ 20, telephony metadata is easy to analyze because it is "structured," or highly ordered. This fact is not unique, however, to telephony metadata. Many other types of data are also structured and are therefore also easy to analyze in the aggregate.

11. Virtually every type of digital communications metadata is structured. This includes, but is by no means limited to, email metadata, Internet-usage history, and Internet chat records. Many other types of records are also structured, including financial records, credit-card records, and even portions of medical records. This is no coincidence: industry experts often develop and agree upon a standardized form for the structure of metadata or transactional data.

12. Most of these sorts of structured records are interconnected. Communications metadata are interconnected in a fairly obvious manner. But the same is true of financial and medical records. For example, prescription records memorialize the identity of the doctor, the identity of the patient, and the medicine prescribed. In a Medicare-fraud investigation, it would be possible to use prescription records to conduct a social-graph analysis, *see* Felten Decl. ¶ 48 (explaining social graphs), of a particular doctor's prescriptions. The analysis might reveal connections between several doctors' prescription habits, their overlapping patients, their connections to other doctors known to engage in fraudulent practices, or divergences between their prescription habits and the prescription habits of other doctors. *See, e.g.*, The Rise of Organized Crime in Health Care: Social Network Analytics Uncover Hidden and Complex Fraud

Schemes, *available at* http://www.writersstudio.com/samples/whitepapers/Lexis%20Nexis%20social%20network%20analytics.pdf.

13. The same sort of social-graph analysis could be applied to financial or credit-card records to uncover organized crime or fraud, because those records are also interconnected. A money-laundering investigation, for instance, could benefit from the ability to trace funds transferred from their source through a series of sham transactions and ultimately back to the original account or owner, in order to make those funds appear "clean."

It would be feasible to quarantine the ACLU's call records.

14. The government states that it would take "approximately six months," Gov't PI Opp. 40, to devise a way in which to quarantine the ACLU's call records if the ACLU's request for a preliminary injunction were granted. This is an implausible estimate for the time necessary to develop the software to quarantine the ACLU's call records.

15. There are a number of ways that the government could efficiently and effectively quarantine the ACLU's call records. For example, the NSA could deploy an automated script that would search its database for the ACLU's call records and move those records to another database that would not be accessed except at the direction of the Court. It could also apply a filter to its three-hop analysis such that any call to or from an ACLU number would be ignored (as would any other call down the chain from any such call). Indeed, it appears that the NSA already has the ability to filter its three-hop analysis to exclude certain phone numbers. *See, e.g.*, David S. Kris, *On the Bulk Collection of Tangible Things*, 1:4 Lawfare Res. Pap. Ser. 1, 13–14 (Sept. 29, 2013) ("NSA technicians may access the metadata to make the data more useable—e.g., to create a 'defeat list' to block contact chaining through 'high volume identifiers'

presumably associated with telemarketing or similar activity." (quoting orders of the Foreign Intelligence Surveillance Court)).

16. Both of these solutions are relatively simple from a technological perspective, and it is difficult to understand how either could take significant resources to implement, much less the six months estimated by the government.

Edward W. Felten

Dated: October 25, 2013