UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

AMERICAN CIVIL LIBERTIES UNION, et al., Plaintiffs, v. FEDERAL BUREAU OF INVESTIGATION, et al., Defendants.	Case No. 1:11-cv-07562-WHP

SUPPLEMENTAL DECLARATION OF JENNIFER L. HUDSON
DIRECTOR, INFORMATION MANAGEMENT DIVISION,
OFFICE OF THE CHIEF INFORMATION OFFICER,
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Pursuant to 28 U.S.C. § 1746, I, Jennifer L. Hudson, declare the following to be true and correct:

1. I am the Director of the Information Management Division ("IMD") of the Office of the Chief Information Officer ("CIO") for the Office of the Director of National Intelligence ("ODNI"). I have held this position since May, 2013. I joined ODNI in 2007 as the Chief, Information Review and Release Branch, and was directly involved in the creation of ODNI's IMD. After a one-year assignment working in the ODNI's Office of Legislative Affairs, I returned to IMD and assumed my current position as the Director of that office. Prior to my arrival in ODNI, I held information management positions in the Joint Personnel Recovery Agency, the Defense Prisoner of War/Missing Persons Office, and later in the Public Access Branch at the Defense Intelligence Agency.

2. IMD is responsible for facilitating the implementation of information management-related Executive orders, laws, regulations, and ODNI policy. This function entails controlling information throughout its life cycle and includes the areas of records management, classification management and declassification, pre-publication reviews, and responding to requests under the Freedom of Information Act ("FOIA") and the Privacy Act ("PA").

3. Under a written delegation of authority by the Director of National Intelligence ("DNI") pursuant to section 1.3(c) of Executive Order ("E.O.") 13526, I hold original classification authority ("OCA") at the TOP SECRET level. I am authorized, therefore, to conduct classification reviews and to make original classification and declassification decisions for intelligence information up to and including the TOP SECRET level. In my current position, I am the final decision-making authority regarding FOIA and PA processing for the ODNI/IMD.

4. Through the exercise of my official duties, I have become familiar with this civil action and the underlying FOIA request. I make the following statements based upon my personal knowledge and information made available to me in my official capacity.

5. I submit this supplemental declaration in further support of the Department of Justice's ("DoJ") Motion for Summary Judgment in this proceeding. It is my understanding that the plaintiffs have narrowed their challenge to "fully withheld opinions or orders of the Foreign Intelligence Surveillance Court that related to bulk collection of any information (i.e., not just telephony metadata)." The U.S. Government has acknowledged that, pursuant to Section 215 of the USA PATRIOT Act ("Section 215"), 50 U.S.C. § 1861, it operates a telephony-metadata intelligence-gathering program under Section 215 as part of its efforts to combat international terrorism. The purpose of this declaration is to address an allegation by plaintiffs in their Cross-Motion for Summary Judgment and Opposition to DoJ's Motion for Summary Judgment.

Plaintiffs cite to a New York Times article and allege that the U.S. Government has also used Section 215 to engage in bulk collection of other kinds of records including international money transfers. As explained further below, the Intelligence Community ("IC") can neither confirm nor deny whether the U.S. Government has or has not used Section 215 in this manner.

6. The IC, through ODNI, can neither confirm nor deny whether the U.S. Government has also used Section 215 to engage in bulk collection of other kinds of records because confirming or denying the existence or nonexistence of such intelligence activities would reveal classified information that is protected from disclosure by Executive order and statute and would reveal intelligence sources and methods. Because the IC can neither confirm nor deny whether the U.S. Government has also used Section 215 to engage in bulk collection of other records other than telephony metadata, the IC can also neither confirm nor deny whether any of the records identified as responsive to the plaintiffs' FOIA request relate to such matters. Nor can the IC confirm or deny whether other records exist relating to such matters, regardless of whether such documents are responsive to the plaintiffs' FOIA request.

7. The IC is charged with carrying out a number of important functions on behalf of the U.S. Government, which include, among other activities, collecting and analyzing foreign intelligence and counterintelligence. A defining characteristic of agency activities within the IC is that they are typically carried out through clandestine means, and therefore, they must remain secret in order to be effective. In the context of FOIA, this means that the IC must carefully evaluate whether its response to a particular FOIA request could jeopardize the clandestine nature of its intelligence activities or otherwise reveal previously undisclosed information about its sources, methods, activities, capabilities, interests, strengths, limitations, weaknesses, resources, etc.

8. After careful review, I have determined that if the IC were to confirm the existence or nonexistence of additional bulk collection activities under Section 215, such confirmation would reveal sensitive information about the IC's intelligence sources, methods, activities, capabilities, interests, strengths, weaknesses, limitations and resources that is properly protected from disclosure by E.O. 13526 and statute. Therefore, the IC, through ODNI, can neither confirm nor deny whether the U.S. Government has also used Section 215 to engage in bulk collection of other kinds of records because the existence or nonexistence of such activities is a currently and properly classified fact and exempt from release under FOIA Exemptions 1 and 3, 5 U.S.C. section 552(b)(1) and (b)(3), the disclosure of which reasonably could be expected to cause damage to the national security.

II. APPLICATION OF FOIA EXEMPTIONS

A. FOIA Exemption 1

9. The explanation for why the records at issue in this case are exempt from disclosure pursuant to Exemptions 1 and 3 is set forth in my prior declaration, dated April 4, 2014. The following paragraphs supplement my earlier declaration.

10. FOIA Exemption 1 provides that FOIA does not require the production of records that are: "(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order." 5 U.S.C. § 552(b)(1).

11. Section 1.1(a) of E.O. 13526 provides that information may be originally classified under the terms of the order only if all of the following conditions are met: (1) an OCA is classifying the information; (2) the information is owned by, produced by or for, or is under the control of the U.S. Government; (3) the information falls within one or more of the categories

of information listed in section 1.4 of E.O. 13526; and (4) the OCA determines that the unauthorized disclosure of the information reasonably could be expected to result in some level of damage to the national security, and the OCA is able to identify or describe the damage.

12. Furthermore, section 3.6(a) of E.O. 13526 specifically states that "[a]n agency may refuse to confirm or deny the existence or nonexistence of requested records whenever the fact of their existence or nonexistence is itself classified under this order or its predecessors." E.O. 13526 therefore explicitly authorizes precisely the type of response that the IC is providing to plaintiffs in this case.

13. Consistent with sections 1.1(a) and 3.6(a) of E.O. 13526, and as described below, I have determined that the existence or nonexistence of additional IC bulk collection activities under Section 215 is a properly classified fact that concerns "intelligence activities . . . [and] intelligence sources or methods," as provided in section 1.4(c) of the Executive Order, this fact is owned by and under the control of the U.S. Government, and the unauthorized disclosure of the existence or nonexistence of such activities reasonably could be expected to result in damage to national security.

14. My determination that the existence or nonexistence of additional IC bulk collection activities under Section 215 is classified has not been made to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interests of national security.

i. Intelligence Activities

15. Clandestine intelligence activities lie at the heart of the mission of the IC. As previously described, an acknowledgment of information regarding the existence or nonexistence

of specific intelligence activities can reveal the IC's specific intelligence sources, methods, activities, capabilities, authorities, interests, strengths, weaknesses, limitations and resources. Terrorist organizations, foreign intelligence services, and other hostile groups use this information to thwart IC activities or exploit perceived or identified weaknesses or limitations and attack the United States and its interests. These parties search continually for information regarding IC activities and are able to gather information from myriad sources, analyze this information, and devise ways to defeat IC activities or exploit perceived or identified weaknesses or limitations from seemingly disparate pieces of information. Even where the subject of an intelligence interest is no longer of interest, adversaries of the U.S. Government continue to seek such information, as such information could suggest to these adversaries how the IC may currently focus its intelligence activities. In this case, acknowledging the existence or nonexistence of additional IC bulk collection activities under Section 215 would reveal intelligence activities and this reasonably could be expected to cause damage to national security"

ii. Intelligence Sources and Methods

16. Intelligence sources and methods include the basic business practices and methodological "tools" used by the IC to accomplish its mission. Intelligence sources and methods must be protected from disclosure in every situation where a certain intelligence interest, capability, or technique is unknown to those groups that could take countermeasures to nullify its effectiveness. Once an intelligence method or its use in a certain situation is discovered, its continued successful use by the IC is jeopardized. Detailed knowledge of each intelligence method must be protected from disclosure because such knowledge would be of material assistance to those who seek to detect, prevent, or damage U.S. intelligence operations.

Likewise, weakness or limitations in the IC intelligence collection capabilities must also be protected from disclosure in order to protect against exploitation by our adversaries. The two examples below will illustrate this.

17. First, if the IC admits that it possesses clandestine intelligence information about particular individuals or organizations, the IC essentially admits that one or more of the target's activities have been detected by the IC. Such an acknowledgment alerts the individuals or organizations as well as other similarly situated individuals or organizations that they must take countermeasures to make future activities undetectable by the IC. If a target's countermeasures are successful, the IC loses its ability to monitor the target's activities. Moreover, others who may be collaborating with such individuals or organizations will soon cease engaging in these detectable activities with similar results. In a case where the individuals or organizations are no longer active, associates are still alerted to the fact that one or more activities may have been detected by the IC, and any benefit from those activities should be considered suspect unless proven otherwise.

18. Second, if the IC denies that it possesses intelligence information about particular individuals or organizations, the IC admits that it has not detected any activities by those individuals or organizations. If those individuals or organizations are ones who indeed should be of intelligence interest to the IC, the IC essentially admits to the individuals or organizations as well as other similarly situated individuals or organizations that their efforts to conceal their activities have been successful. The result of the IC's admission is that the individuals or organizations would know that they could continue to act with impunity. Moreover, associates of the individuals or organizations, along with other intelligence operatives or terrorists, could soon begin to emulate the same successful pattern of undetectable activities with similar results.

In a case where the individuals or organizations are no longer active, acknowledging an absence of IC records would signal to the individuals or organizations, and associates, that their activities were never detected by the IC, and any ongoing benefit of those activities can continue to be reaped.

19. Finally, the effective collection and analysis of intelligence requires the IC to prevent disclosing to our adversaries the specific persons and areas in which the IC is interested and upon which it focuses its methods and resources. Every country or group has limited resources. The disclosure to U.S. adversaries of whether the IC uses a particular authority to collect certain information would indicate to our adversaries how the IC is allocating its resources. Therefore, these individuals or organizations may array their counterintelligence and security resources in a manner most efficiently designed to frustrate the IC's use of that authority. The more efficiently an intelligence target may apply its counterintelligence resources, the more likely it will deny the information of interest to the United States.

20. Similarly, in this case, acknowledging the existence or nonexistence of additional IC bulk collection activities under Section 215 reasonably could be expected to cause damage to the national security by alerting individuals or organizations of intelligence interest to what methods the IC employed or did not employ with regard to bulk collection, thus allowing those individuals or organizations to determine whether and what countermeasures to make in the future to thwart IC intelligence collection and activities. Thus, this information is currently and properly classified, and consequently, it is exempt from disclosure under FOIA Exemption 1.

B. FOIA Exemption 3

21. FOIA Exemption 3 provides that FOIA does not apply to matters that are:

> specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the

> public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld . . . .

5 U.S.C. § 552(b)(3).

22. Section 102A(i)(1) of the National Security Act of 1947, as amended, 50 U.S.C. § 3024(i)(1) (the "National Security Act"), provides that the DNI "shall protect intelligence sources and methods from unauthorized disclosure." Accordingly, the National Security Act constitutes a federal statute which "requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue." 5 U.S.C. § 552(b)(3). As explained above, acknowledging the existence or nonexistence of additional IC bulk collection activities under Section 215 would reveal information that concerns intelligence sources and methods, which the National Security Act is designed to protect.

23. Accordingly, the fact of the existence or nonexistence of additional IC bulk collection activities under Section 215 is exempt from disclosure under FOIA Exemption 3 pursuant to the National Security Act. In contrast to E.O. 13526, this statute does not require the IC to identify and describe the damage to the national security that reasonably could be expected to result should the IC confirm or deny the existence or nonexistence of additional IC bulk collection activities under Section 215. Nonetheless, I refer the Court to paragraphs 13-20 above for a description of the damage to the national security should the existence or nonexistence of such activities be confirmed or denied. FOIA Exemptions 1 and 3 thus apply independently and co-extensively to plaintiffs' allegation.

CONCLUSION

I certify under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Executed this 30th day of May, 2014

Jennifer L. Hudson
Director, Information Management Division
Office of the Chief Information Officer
Office of the Director of National Intelligence