Pepper Hamilton LLP
Attorneys at Law

CLIENT ALERT

May 19, 2015

Second Circuit Rules PATRIOT Act Does Not Authorize Government's Bulk Telephone Metadata Collection Program

Angelo A. Stio III | stioa@pepperlaw.com
Eli Segal | segale@pepperlaw.com

The ruling is a significant development in the executive, legislative and judicial struggle to strike the right balance between protecting privacy and protecting national security.

Executive Summary

In yet another reminder of the importance of maintaining the privacy of personal information, the Second Circuit Court of Appeals, in *ACLU v. Clapper*, issued a unanimous decision striking down the National Security Agency's bulk collection of telephone records from millions of Americans as an unauthorized exercise of executive power. The decision,

which had its genesis in Edward Snowden's disclosure of the U.S. government's spying efforts, is a significant development in the executive, legislative and judicial branches' efforts to balance the personal privacy of American citizens with national security. A discussion of this important decision and the arguments raised by the U.S. government and by the American Civil Liberties Union and the New York Civil Liberties Union is below.

If you have any questions about the *ACLU v. Clapper* decision or any other data privacy and security issues that impact your organization, attorneys in Pepper Hamilton's Privacy, Security and Data Protection Practice Group have the knowledge and experience to assist you.

Introduction

On June 5, 2013, Edward Snowden, via *The Guardian*, disclosed the existence of the U.S. government's bulk telephone metadata collection program, under which Verizon was ordered to provide the National Security Agency (NSA), on a daily and ongoing basis, all telephone metadata for all calls made or received in the United States. Just six days later, in the Southern District of New York, the American Civil Liberties Union (ACLU) and the New York Civil Liberties Union (NYCLU) — both Verizon customers — sued the government officials responsible for the program on statutory and constitutional grounds. On May 7, 2015, a unanimous panel from the U.S. Court of Appeals for the Second Circuit shot down the government's statutory justification for the program, holding that the section of the PATRIOT Act that the government claimed authorized its bulk collection of telephone metadata did no such thing. Although the relevant statutory provision is due to sunset at the end of the May 2015, and the court did not address the constitutionality of the program, the Second Circuit's ruling is nonetheless a significant development in the executive, legislative and judicial struggle to strike the right balance between protecting privacy and protecting national security.

The Program and Its Practical and Statutory Justifications

In 1978, in response to allegations of government abuse of warrantless electronic surveillance in the name of national security, Congress passed the Foreign Intelligence Surveillance Act (FISA). FISA established the Foreign Intelligence Surveillance Court (FISC) as a neutral arbiter to rule on government applications to conduct electronic surveillance. In general, however, FISC proceedings are *ex parte* — the court only hears from the government — and secret.

In the wake of September 11, 2001, Congress passed the PATRIOT Act, which, among

other things, amended FISA to enhance the tools available to the government to combat terrorism. One such FISA amendment, section 215 of the PATRIOT Act, permits the FBI director or his designee "to make an application [to the FISC] for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." 50 U.S.C. § 1861(a)(1). That application must include "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." *Id.* at § 1861(b)(2)(A). Thus, stripped to its essence, section 215 permits, with prior authorization by the FISC, the collection of any "tangible things" that are "relevant" to an "authorized" terrorism or intelligence "investigation."

Since at least May 2006, with section 215 as the statutory basis, the U.S. government has been collecting telephone metadata — including originating phone numbers, terminating phone numbers, call times and call lengths — from telephone service providers in bulk. The program's purpose is to create a telephone metadata repository to assist with terrorism and intelligence investigations going forward. Specifically, if the government demonstrates to the FISC that it has a reasonable, articulable suspicion that a particular number is associated with an international terrorism organization, the government can then search the repository it has amassed for metadata associated with that number and for metadata associated with those who have been in contact with that number.

'Irreconcilable with the Statute's Plain Text'

In the suit they filed to challenge the program, the ACLU and NYCLU maintained that (1) the telephone metadata collected in bulk were not "relevant" to any "authorized investigation," as required by section 215; (2) the bulk collection of metadata constituted an unreasonable search in violation of the Fourth Amendment; and (3) the tracking of telephonic associations infringed on the First Amendment's right to free association. The trial court rejected all three arguments and dismissed the complaint. First, the trial court held that the program satisfied section 215's "relevance" requirement, stressing that "[n]ational security investigations are fundamentally different from criminal investigations" in that "[t]hey are prospective — focused on preventing attacks — as opposed to the retrospective investigation of crimes." *ACLU v. Clapper*, 959 F. Supp. 2d 724, 748 (S.D.N.Y. 2013). Second, the trial court ruled that the Fourth Amendment claim failed because, in the

court's view, there could be no reasonable expectation of privacy in telephone metadata created by, or provided to, a third-party service provider. Third, the trial court rejected the First Amendment claim, deeming the plaintiffs' fear that the government would use the repository to identify those with whom they associate too speculative.

Reversing the district court's dismissal of the suit, the Second Circuit roundly rejected the government's and the trial court's reading of section 215 as authorizing the bulk collection of telephone metadata. The court reasoned that the program simply could not be squared with section 215's requirement that records ordered to be produced under the statute be "relevant to an authorized investigation":

> [T]he government takes the position that the metadata collected — a vast amount of which does not contain directly "relevant" information, as the government concedes — are nevertheless "relevant" because they may allow the NSA, at some unknown time in the future, utilizing its ability to sift through the trove of irrelevant data it has collected up to that point, to identify information that *is* relevant. We agree with appellants that such an expansive concept of "relevance" is unprecedented and unwarranted.
>
> *ACLU v. Clapper*, No. 14-42-cv, slip op. at 59 (2d Cir. May 7, 2015).

In addition, the Second Circuit emphasized that the far-reaching nature of the program made express legislative authorization all the more important before giving the program a judicial seal of approval. As the court explained, although "[s]earch warrants and document subpoenas typically seek the records of a particular individual or corporation under investigation, and cover particular time periods when the events under investigation occurred[, t]he orders at issue here contain no such limits." *Id.* at 60–61. Indeed, the court underscored, "[t]he metadata concerning *every* telephone call made or received in the United States using the services of the recipient service provider are demanded, for an indefinite period extending into the future." *Id.* at 61. Thus, given the program's extraordinary sweep, the court found particularly striking the lack of any clear indication that Congress intended to authorize it:

> Such expansive development of government repositories of formerly private records

> would be an unprecedented contraction of the privacy expectations of all Americans. Perhaps such a contraction is required by national security needs in the face of the dangers of contemporary domestic and international terrorism. But we would expect such a momentous decision to be preceded by substantial debate, and expressed in unmistakable language. There is no evidence of such a debate in the legislative history of § 215, and the language of the statute, on its face, is not naturally read as permitting investigative agencies, on the approval of the FISC, to do any more than obtain the sorts of information routinely acquired in the course of criminal investigations of "money laundering [and] drug dealing."
>
> Id. at 74–75.

Because the Second Circuit ruled for the ACLU and NYCLU on statutory grounds, it did not reach their First or Fourth Amendment arguments.

What It Means Going Forward

The Second Circuit's ruling certainly would be more significant had the court ruled on the plaintiffs' constitutional claims, but the opinion is still an important development in the data privacy arena for at least three reasons. First, section 215 is due to sunset on June 1, 2015. Given the Second Circuit's ruling, congressional supporters of the bulk metadata collection program now cannot, with any degree of comfort, simply push for the reauthorization of section 215 as is. Instead, for the program to continue on solid statutory footing, Congress would have to amend section 215 to authorize the program in "unmistakable language" —language that would no doubt be the subject of much heated legislative debate. Second, the Second Circuit's ardent rejection of the government's broad reading of the term "relevant" makes suspect any other investigative efforts — national security–related or not — premised on the theory that information qualifies as "relevant" as long as it might become relevant at some point in the future. Third and finally, the Second Circuit's opinion sends a powerful message that courts will scrutinize government data collection programs — even in the face of national security justifications.