UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

IN RE APPLICATION OF THE FEDERAL BUREAU OF INVESTIGATION FOR AN ORDER REQUIRING THE PRODUCTION OF TANGIBLE THINGS

Docket No. Misc. 14-__

MOTION OF THE CENTER FOR NATIONAL SECURITY STUDIES FOR LEAVE TO FILE BRIEF OF AMICUS CURIAE NOT EXCEEDING 7000 WORDS

On December 18, 2013, this Court granted the Center for National Security Studies ("CNSS") leave to file an amicus brief in the miscellaneous docket making arguments against the legality of the current program of bulk collection of telephony metadata under Section 501 of the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1861. *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, BR 13-158 (Dec. 18, 2013) (McLaughlin, J.). Relying on Fed. R. App. P. 29 for general guidance as to amicus filings., *see id.* at 6 & n.3, the Court set a page limit of 15 pages for this filing.

CNSS hereby moves for leave to file the attached brief, which is less than 7000 words in length. It does so for two reasons. First, 7000 words is the alternative to a 15-page limit provided in Federal Rules of Appellate Procedure. *See* Fed. R. App. P. 29(b) (amicus brief may not exceed half the permitted length of parties' principal briefs); Fed. R. App. P. 32(a)(7) (allowing parties to file briefs up to 30 pages or 14,000 words, at their choice).

Second, it has proved difficult, despite our good faith efforts, to limit our discussion to 15 pages, given the number and substantiality of different legal issues that the Court authorized us to cover. The brief discusses developments involving the telephony metadata collection program since December, showing why this brief is still legally significant, analyzes the history and

requirements of Section 501 more fully than any presentation yet made on a public record in this Court, and does the same for the question of ratification-by-renactment, both with respect to applicable decisions of the United States Supreme Court and other federal courts as well as the implications for democratic governance of the use of the doctrine in this matter. Unlike in the usual case, this amicus brief is not merely supplementing a party's brief. It is the only brief filed in this Court arguing against the lawfulness of the program under Section 501.

Undersigned counsel spoke with counsel for the United States about whether they support or oppose this motion, and they have no position either way.

WHEREFORE, CNSS respectfully requests leave to file the attached brief.

April 3, 2014

Respectfully submitted,

Michael Davidson, D.C. Bar No. 449007
3753 McKinley Street, NW
Washington, DC 20015
(202) 362-4885
mdavid2368@aol.com

Of Counsel

Paul M. Smith, D.C. Bar No. 358870
Michael T. Borgia, D.C. Bar No. 1017737
Jenner & Block, LLP
1099 New York Avenue, N.W.,
Suite 900
Washington, DC 20001
(202) 639-6000 (telephone)
(202) 639-6066 (fax)

Kate A. Martin, D.C. Bar No. 949115
Center for National Security Studies
1730 Pennsylvania Ave., N.W., S. 700
Washington, D.C. 20006
(202) 721-5650 (telephone)
(202) 530- 0128 (fax)
kmartin@cnss.org

Joseph Onek, D.C. Bar No. 43611
The Raben Group
1640 Rhode Island Ave., N.W., S. 600
Washington, D.C. 20036
(202) 587-4942 (telephone)
(202) 463-4803 (fax)
jonek@rabengroup.com

Counsel for Movant Center for National Security Studies

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

IN RE APPLICATION OF THE FEDERAL BUREAU OF INVESTIGATION FOR AN ORDER REQUIRING THE PRODUCTION OF TANGIBLE THINGS

Docket No. Misc. 14-__

BRIEF OF AMICUS CURIAE CENTER FOR NATIONAL SECURITY STUDIES ON THE LACK OF STATUTORY AUTHORITY FOR THIS COURT'S BULK TELEPHONY METADATA ORDERS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

LEGISLATIVE MATERIALS

OTHER AUTHORITIES

INTEREST OF AMICUS AND CONTINUED RELEVANCE OF QUESTION PRESENTED

The Center for National Security Studies ("the Center") is a project of the National Security Archive Fund, Inc., a tax-exempt organization. Founded in 1974, the Center is dedicated to the defense of civil liberties, human rights, and constitutional limits on government power. A principal concern of the Center is the prevention of illegal government surveillance. On December 18, 2013, in an order entered in BR 13-158, this Court granted the Center leave to file an amicus curiae brief explaining why Section 501 of the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1861, does not authorize the bulk collection by the National Security Agency ("NSA") of metadata on the calls, including local calls, of virtually all Americans, a program that the Solicitor General has described to the Supreme Court as the Telephony Records Program ("the program").[1] Per the Court's order, this brief will be placed in a miscellaneous docket for consideration by any judge when considering a future application.

Since December, the President has undertaken initiatives to limit how the government collects and searches the telephony metadata while preserving the program's intelligence capabilities. In response to the government's motion, on February 5, 2014, this Court entered an order modifying provisions relating to NSA's queries of telephony metadata, but not modifying the collection of it. On March 27, 2014, the President issued a statement "that the government should not collect or hold this data in bulk" and that he was seeking legislation to implement his proposal. However, the President also directed the Department of Justice to seek from this Court a 90-day reauthorization of the existing program, as modified in February. On March 28, it was announced that this Court had granted an extension until June 20, 2014. More such extension

[1] While the Center recognizes that the NSA's bulk collection raises significant issues under the Fourth Amendment and the Electronic Communications Privacy Act, this brief does not address those issues.

requests are possible. Accordingly, the question whether Section 501 authorizes the NSA's bulk collection of telephony metadata remains legally important.

Moreover, regardless of any changes ultimately made to the program, this Court's opinions approving the program in its current form will not become a dead letter. Those opinions could be invoked in future cases concerning a number of important issues, such as the limits of "relevance" as applied to large-scale government surveillance. *See infra* Section II.d. Future invocation of this Court's holding that Congress implicitly ratified the Court's and the Executive Branch's secret interpretation of Section 501, *see infra* Section III, could also have significant ramifications for questions about open government and congressional action far beyond this specific context. *See Korematsu v. United States*, 323 U.S. 214, 246 (1944) (Jackson, J. dissenting) (warning against the judicial validation of a principle that "lies about like a loaded weapon[,] ready for the hand of any authority that can bring forward a plausible claim of an urgent need").

Given the important issues raised by this Court's orders authorizing the program, the Center respectfully submits this brief pursuant to the leave granted by this Court.

ARGUMENT

I. Introduction

Congress has never authorized the telephony metadata program. Congress did not authorize the program in Section 501, as the program violates the plain text of Section 501 and is inconsistent with the structure of that section and FISA as a whole. *See infra* Section II. Nor can Congress be deemed to have secretly ratified the program in 2011 when extending the sunset of Section 501 to June 2015. *See infra* Section III. Finding otherwise requires an unprecedented extension of the ratification-by-reenactment doctrine, and is fundamentally inconsistent with principles of democratic government. When the government acts in an area of questionable

constitutionality, Congress cannot be deemed to have authorized that action by mere implication or acquiescence. *Greene v. McElroy*, 360 U.S. 474, 506-07 (1959). Rather, Congress must explicitly indicate that it intends to alter the rights and limitations normally afforded by the law. *Id.* Yet neither in the text of Section 501 nor in the extension of the sunset has Congress made such an explicit statement.

Although the issues addressed here principally involve statutory interpretation, it must be recognized that much more is at stake than simply the correct interpretation of one statute. As both the president's Review Group and the Privacy and Civil Liberties Oversight Board ("PCLOB") recognized in their reports on the program, records of an individual's calls made over a period of years can reveal detailed information about that person's activities and associations. Government collection of such information can be expected to chill protected First Amendment activities, as well as fundamentally shift the balance of power between the government and the American public. *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies* 116-17 (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (citing *United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring)); David Medine et al., Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted Under Section 215 of the USA PATIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* 156 (2014), *available at* http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf.

This Court should recognize the importance of requiring Congress to act first to strike the balance between privacy and national security in the novel and complex circumstances now present. As Justice Alito observed in *United States v. Jones*: "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." 132 S. Ct. 945, 964 (2012) (internal citation omitted). As discussed in detail throughout this brief, Congress has neither authorized the program nor enacted a statutory scheme designed to govern mass collection of bulk telephony metadata. Yet, the rulings of this Court have allowed the executive branch and the judiciary to assume that legislative role. In its first opinion on bulk metadata collection (approving collection of bulk Internet metadata in 2004), this Court, rather than recognize the absence of express congressional authorization or a robust statutory scheme that balances the relevant interests, emphasized the deference that it thought should be given to executive branch assessments and responses to national security threats and in determining the potential intelligence significance of information. Opinion and Order of Presiding Judge Kollar-Kotelly, Docket No. PR/TT (redacted), at 30. But the executive branch has no special competence entitling it to deference in weighing the privacy interests of Americans with regard to the creation of massive government databases of the records of ordinary activity like emails and telephone calls. And while the judicial branch has the responsibility of determining whether the Fourth Amendment prohibits that collection or requires a warrant, it is for Congress in the first instance to make a legislative judgment about the appropriate balance between national security and individual privacy and security in a collection program of such size and duration.

II. Section 501 Does Not Authorize the Program.

Section 501 permits the FBI Director to move the FISA Court for an order "requiring the production of any tangible things (including books, records, papers, documents, and other items) . . . ." 50 U.S.C. § 1861(a)(1). Those tangible things must be "for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." *Id.* An application under Section 501 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*, " *id.* § 1861(b)(2)(A) (emphasis added), and "an enumeration of the minimization procedures . . . that are applicable to the retention and dissemination" by the FBI of the tangible things produced, *id.* § 1861(b)(2)(B). An order granted by the Court under Section 501 must be limited to tangible things that "can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation" or other court order. *Id.* § 1861(c)(2)(D).

A walk through these provisions—with attention paid both to what is present and what is absent—shows that Section 501 does not authorize the NSA's bulk collection of telephony metadata. Specifically, the program cannot be reconciled with Section 501 because that section: (a) is explicitly directed to the FBI, not the NSA; (b) only allows production of tangible things for particular authorized investigations, not an amalgam of all current and potential future investigations; (c) requires that the tangible things be "relevant" to authorized investigations; (d) is limited to tangible things that can be obtained by a grand jury subpoena or other court order; and (e) unlike other sections of FISA that were designed to accommodate ongoing or bulk collection, contains no provision to regulate continuous collection.

A. Section 501 Is Explicitly Directed to the FBI, not the NSA.

In contrast to other FISA provisions, Section 501 is directed explicitly to a single government entity—the FBI.[2] *See* 50 U.S.C. § 1861(a)(1). Depending on the sensitivity of categories of records, Congress has prescribed in Section 501 for levels of authority among officials ***within*** the FBI for the making of applications, 50 U.S.C. § 1861(a)(1), (a)(2) and (a)(3), but in no way has provided for any authority outside of the FBI. The orders authorized by Section 501 are expressly similar to subpoenas and other court orders, *see infra* Sections II.C.-D., and in fact impose an additional level of supervision by requiring Court approval before issuance. Such orders are familiar tools of the investigatory activities performed by the FBI. Congress's decision to place authority under Section 501 in the FBI, rather than in any other government agency including the NSA, indicates that Congress never intended that section to be the foundation of the NSA's bulk collection program sweeping in massive amounts of domestic call data.[3]

Congress's explicit and exclusive placement of Section 501 authority in the FBI was both sensible and significant. Section 501 orders are addressed to businesses within the United States about the transactions of persons within the United States, and therefore are likely to present questions about constitutional and statutory authority relating to persons in the United States. It is both important and unsurprising that in Section 501 Congress vested that authority exclusively

---

[2] For instance, a "Federal officer" may apply for electronic surveillance orders under Title I or search orders under Title II. 50 U.S.C. §§ 1804(a), 1823(a).

[3] Other provisions of Title V make plain that the FBI cannot be just a nominal applicant on behalf of the NSA. The FBI's responsibilities go beyond the making of the initial application and extend throughout Section 501. Both the minimization and the use provisions of Section 501 apply to records "received" by the FBI. Section 501(g) and (h), 50 U.S.C. § 1861(g) and (h). Section 501 places the FBI Director at the center of procedures for disclosure of information about business records orders. Section 501(d), 50 U.S.C. § 1861(d).

in an entity that operates directly under the Attorney General, and that is experienced with domestic investigations.

Moreover, Congress's decision to direct Section 501 to the FBI reflects a long-standing policy of limiting the scope of foreign intelligence operations in the domestic sphere. The Director of National Intelligence has the responsibility, under section 102A(g) of the National Security Act of 1947, "to ensure maximum availability of and access to intelligence information within the intelligence community consistent with national security requirements." 50 U.S.C. § 3024(g). But that key objective in no way diminishes the need for faithfulness to fundamental decisions by the Congress on important boundaries. Thus, the Director of the Central Intelligence Agency "shall have no police, subpoena, or law enforcement powers or internal security functions." 50 U.S.C. § 3036(d)(1). Congress also proscribes the use of the U.S. military to execute the laws "except in cases and under circumstances expressly authorized by the Constitution or Acts of Congress." 18 U.S.C. § 1385. Congress's express determination in Section 501 to grant authority regarding business records to the FBI, and not the NSA, constitutes a similar limitation on the role of intelligence/military organizations concerning domestic activity.

The National Security Agency is tasked to perform foreign intelligence responsibilities that are essential to our Nation's security. The Agency is strengthened when Americans are assured that its powerful tools are directed outward not inward but it is weakened when thrust into the role of analyst and archivist for the details of calls of all Americans. Adherence to the plain text of Section 501 would prevent that harm.

B. Section 501 Only Allows for Collection of Tangible Things for Specific Investigations.

When interpreting Section 501, as with any other statute, the Court must give effect to all the relevant language and may not adopt a reading that renders certain language meaningless. *See Bilski v. Kappos*, 130 S. Ct. 3218, 3228 (2010). This Court's rulings approving the program have violated this rule because they effectively nullified the requirement that the tangible things collected be relevant to "an authorized investigation."

When the bulk records are collected, the collection is not tied to any terrorism investigation. Rather, the government has argued and this Court has accepted that Section 501 permits the collection to be tied simply to *any* investigation, including investigations that may arise in the future. But it is clear that Section 501 requires such a connection at the time of collection. For example, Section 501 requires that the investigation to which the records are relevant be conducted under approved guidelines and not based solely on First Amendment protected activities. Additionally, the authorized investigation must be made under guidelines established by the Attorney General. A determination whether an investigation meets those requirements cannot be made for bulk collection, since the collection is not tied to any identified investigation.

C. Section 501 Requires that Collection be "Relevant" to Authorized Investigations.

The records collected by the program also cannot be considered "relevant" to an authorized investigation in any familiar or meaningful sense of that term. The program involves bulk collection far broader than has been permitted in analogous legal contexts, and effectively reads that phrase out of the statute, given that there is no apparent principle to differentiate those records that are within the scope of collection from those that are not. Perhaps even more problematic is the government's effort to justify the program's vast collection by dramatically

redefining "relevance." Under the government's view, relevance is to be transformed from a limit on the government's authority to collect information about Americans, based on what is justified by the facts and circumstances of the investigation, into a blank check permitting the government to collect as much personal information as its mass surveillance tools and methods permit.

As the government has noted, the requirement that the tangible things collected be "relevant" to an authorized investigation reflects a familiar limitation on the government's ability to collect records on Americans, and is routinely applied to define the permissible scope of subpoenas duces tecum issued by grand juries and administrative agencies. *See* Administration White Paper, *Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT ACT* 1-2, 9-11 (Aug. 9, 2013), *available at* http://i2.cdn.turner.com/cnn/2013/images/08/09/administration.white.paper.section.215.pdf (hereinafter "White Paper"). That requirement was added to FISA's tangible things provision by the USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006). Those 2006 amendments clarified the limitations of the broadly worded tangible records provision enacted by the USA PATRIOT Act, shortly after September 11, 2001.

A relevance requirement cannot be defined only by hard-and-fast rules. *See In re Subpoena Duces Tecum*, 228 F.3d 341, 347 (4th Cir. 2000) (stating that "relevance" varies according to the "nature, purposes, and scope of the inquiry," and "cannot be reduced to formula." (quoting *Okla. Press Publ'g Co. v. Walling*, 327 U.S. 186, 209 (1946))). Rather, "relevance" is a flexible, fact-intensive standard that differentiates between what is within the scope of and reasonably related to a particular inquiry and the rest of the universe of existing documents and information. *See United States v. Matras*, 487 F.2d 1271 1274-75 (8th Cir. 1973)

(refusing to enforce an IRS summons where the IRS argued that it needed to obtain an expansive amount of information to provide a "road map" for its investigation). Although lines between what is relevant and what is not often cannot be drawn with precision, the basic notion of relevance is that some line must exist. *See United States v. R. Enters., Inc.*, 498 U.S. 292, 299 (1991) (the investigatory power of a grand jury is "not unlimited" and cannot be used "to engage in arbitrary fishing expeditions."); *EEOC v. United Air Lines, Inc.*, 287 F.3d 643, 653 (7th Cir. 2002) (the term "relevant" should not be interpreted so broadly as to render the statutory language a "nullity" (quoting *EEOC v. Shell Oil Co.*, 466 U.S. 54, 69 (1984))); *RNR Enters., Inc. v. SEC*, 122 F.3d 93, 97 (2d Cir. 1997) (a subpoena "may be of such a sweeping nature and so unrelated to the matter properly under inquiry as to exceed the investigatory power" (quoting *United States v. Morton Salt Co.*, 338 U.S. 632, 652 (1950))).

But the NSA's bulk collection under Section 501 eliminates the distinction between what is relevant and what is not. The government never even asserts that particular facts or circumstances, such as the activities being investigated or the targets of the investigation, suggest that certain records may be relevant. To the contrary, because the records are collected on an ongoing basis, the government is not even claiming relevance at the time the records are collected. The government simply claims that because a very small number of calls made by Americans may be relevant to a terrorism investigation, it is entitled to collect and review all the call data of all Americans in perpetuity.

The government notes that terrorism investigations often are very large, and that large subject matters have justified very broad subpoenas. Those observations are undoubtedly true, and it is also true that subpoenas and court orders frequently require the production of large numbers of records, even where it is clear that many of the records produced ultimately will not

prove to be important. *See In re Grand Jury Proceedings*, 616 F.3d 1186, 1205 (10th Cir. 2010) ("Incidental production of irrelevant documents . . . is simply a necessary consequence of the grand jury's broad investigative powers . . . ."). Of course it must be acknowledged—as the government does—that the case law defining the permissible scope of "relevance" was developed in response to far more limited subpoenas and orders than what is at issue here. White Paper at 11 ("To be sure, the cases that have been decided in these contexts do not involve collection of data on the scale at issue in the telephony metadata collection program, and the purpose for which information was sought in these cases was not as expansive in scope as a nationwide intelligence collection effort designed to identify terrorist threats."). Those cases provide tenuous support for the unparalleled breadth of collection at issue here.

More fundamentally, the fatal flaw of the program is not that the number of records collected is large *per se* (although the incredible breadth of the records collected certainly illustrates the program's unrestrained nature). The question of relevance ultimately is not just one of quantity, but also of quality. The program's fatal flaw is that it simply collects the records of millions of Americans in bulk continuously without providing any way to plausibly connect the vast majority of records collected to an investigation, or to differentiate between the records that may be relevant and those that are not. Where a doctor allegedly committed fraud related to 15,000 patients' records, the grand jury would be justified in subpoenaing the records of all 15,000, notwithstanding the large number of records involved. *See In re Subpoena Duces Tecum*, 228 F.3d at 350-51. However, the grand jury would not be justified in subpoenaing the records of all doctors perpetually without limitation to see if others had committed or would commit fraud too. In short, the government's applications here stretch the relevance standard so far that it becomes a legal "nullity." *United Air Lines*, 287 F.3d at 653.

In order to shoehorn this massive collection into the familiar concept of relevance, the government has proffered a novel theory: that while the vast majority of the bulk metadata is not relevant to any facts or circumstances of any authorized investigation, it is relevant to investigative *tools* employed by NSA—specifically, to data analytical tools used to determine patterns and connections between different numbers, thereby revealing associations between suspects. *See* White Paper at 12-13.

While this rhetorical shift—from relevance as determined by the circumstances of the inquiry to relevance as determined by the government's investigative tools—may seem subtle, its consequences are dramatic. On the government's view, the relevance standard does not work to limit the permissible scope of data collection to what the government actually needs for a specific investigation, but rather functions as an elastic statutory term whose meaning expands, by virtue of a kind of blank check from Congress, as information technology provides ever more powerful tools for agencies of the executive branch to identify matters of interest in masses of information about ordinary conduct, such as the calls of all Americans. The government's argument does not justify smaller or greater amounts of collection depending on the actual scope of an investigation; for all terrorism investigations, regardless of size, scope or complexity, the nation's telephony metadata is apparently always "relevant." On the government's view, it is sufficient that the data is stored in bulk and can be analyzed effectively by the NSA. In this way, a limitation that was added in 2006 to clarify the *limits* of the 2001 amendments actually serves as an invitation for unfettered collection of records on all Americans' activities.

The potential consequences of this argument beyond the telephony metadata program are substantial. That argument can readily be applied to justify the collection of virtually any kind of data that can be classified as a "business record," such as location information, and credit card

and other financial transactions within the United States, in connection with any current or potential future investigation. And, if the government is correct that the term "relevance" in Section 501 carries the same meaning as it does for grand jury and administrative subpoenas, the permissible scope of any of the many hundred authorities in the United States Code for judicial or administrative subpoenas can expand far beyond the size and scope of any specific investigation so long as advanced analytical tools can be used to search bulk data for relevant information. *See, e.g.*, FISC Supplemental Order of November 23, 2010 (BR 10-82) (released March 28, 2014) (noting that the term "relevance" governs production of financial records under the Right to Financial Privacy Act, 12 U.S.C. 3401, *et seq.*).

Perhaps recognizing the absence of a limiting principle, the government suggests that telephony metadata may be uniquely conducive to the NSA's analytic techniques, and therefore that other forms of data collected in bulk may not be considered "relevant" to those techniques. White Paper at 14. But that bald assertion fails to account for the extraordinary power and growth of data analytics in both the public and private sectors. Public and private entities are continuously finding novel ways to learn more comprehensive and detailed information about individuals' activities, preferences, habits, associations, etc. Even assuming that the government does not currently have a productive way to analyze other types of data in bulk, such as geolocation data or financial transactions, it is far from impossible that the government will develop such a mechanism in the future.

D. Section 501 Is Limited to Tangible Things that Can Be Obtained by a Grand Jury Subpoena or Other Court Order.

Along with the relevance requirement, the 2006 amendments added several other restrictions under the heading "Additional Protections," Pub. L. No. 109-177, § 106(d), 120 Stat. at 197. One is a provision limiting the permissible scope of a production order by the FISA Court

"only" to tangible things that could be obtained by a subpoena from a federal court, including a subpoena duces tecum issued by a grand jury. 50 U.S.C. § 1861(c)(2)(D). The government cites the provision limiting the scope of collection to records that could be obtained via grand jury subpoena or court order, 50 U.S.C. § 1861(c)(2)(D), as evidence that Congress intended Section 501 to authorize very broad collection. But that interpretation ignores both the text of that provision and legislative history surrounding its addition in 2006. That provision was intended to act as a shield against excessive collection, not, as the government would have it, a sword authorizing virtually limitless collection. The provision states that the government may collect "only" the records that could be obtained by those other means, and was added by the 2006 amendments under the title "Additional Protections." Pub. L. No. 109-177, § 106(d), 120 Stat. at 197. As discussed above, the program far exceeds the scope of collection authorized by grand jury subpoenas and court orders. Moreover, the government fails to appreciate why that provision was added—not to broaden the scope of collection, but to ensure that privileges and other protections that limited the permissible scope of collection in other contexts also applied to Section 501. A version of that limitation was discussed in a report of the Senate Intelligence Committee, S. Rep. No. 109-85 (2005), and prohibited collection of "privileged" records. Another version was included in a bill drafted by the Senate Judiciary Committee and passed as H.R. 3199 (2005), and prohibited collection of "protected" records. This history indicates that the provision was added to ensure that the tangible records contemplated by Section 501, including library records, book-seller records, health records, gun sale records, etc. could not be collected in violation of established rights and privileges.