Counterintelligence and Access to Transactional Records: A Practical History of USA PATRIOT Act Section 215

Michael J. Woods

The USA PATRIOT Act has sparked intense public debate, with proponents claiming that the Act is a necessarily hard-minded response to a national crisis, while opponents see unwarranted, even opportunistic, expansion of state power. Perhaps no provision of the Act has generated more controversy than §215, which authorizes the FBI to seek a court order compelling the production of “any tangible things” relevant to certain counterintelligence and counterterrorism investigations. Like many other provisions of the USA PATRIOT Act, §215 will expire on December 31, 2005, unless reauthorized by Congress. The controversy, therefore, is likely to intensify over the coming months.

The rhetoric swirling about this provision has been extreme, despite the paucity of evidence that it has ever actually been used — which suggests that the section is neither the deadly threat to civil liberties nor the vital operational...
necessity that its detractors and defenders, respectively, contend. Section 215, removed from its context in national security law, might be regarded as ominous, but placed in the larger context of operational counterintelligence authorities for access to transactional information, §215 emerges as an understandable, though arguably incomplete, evolutionary step. This article is intended to supply that context, and then to examine both criticism and potential revisions of §215.

The difficulty in accomplishing this task is that, as in so many discussions of national security law, the practical relationship and functional roles of the various legal authorities are embedded in government operations that remain classified. Because few counterintelligence operational authorities have been the subject of litigation, debates over these authorities tend to occur on a theoretical level, with outsiders parsing the statutory text and gleaning clues from what little exists in public records, and with insiders limiting themselves to high-level policy talk bereft of any concrete details. Since September 11, 2001, however, the FBI and the Department of Justice have declassified and released a number of key documents in response to various inquiries, investigations, and lawsuits. I believe that enough information now exists in the public domain to allow an “insider” to convey a reasonably accurate picture of §215’s evolution using open source material.

In Section I, I will provide an overview of pre-USA PATRIOT Act authorities governing counterintelligence access to transactional information. In Section II, I will discuss the creation of §215 and address some of the principal concerns raised by critics of the USA PATRIOT Act. Finally, in Section III, I will examine potential modifications or alternatives to §215 as it currently exists.

7. In this article I sometimes refer to procedures for obtaining certain information as “authorities,” since that term is used within the Federal Bureau of Investigation as shorthand for the statutory or regulatory authorization pursuant to which intelligence operations are conducted.


10. All the factual material in this article comes from publicly available documents, as indicated throughout. No reference to any classified material is intended.
I. AN OVERVIEW OF COUNTERINTELLIGENCE OPERATIONAL AUTHORITIES

A full understanding of §215 begins with the role of counterintelligence within the larger landscape of national security law. National security law includes a range of authorities granted to the executive branch for the defense of the nation from foreign powers. These legal authorities, subject to congressional regulation and oversight, are the basis for military operations, the collection of foreign intelligence, and covert activities. “Counterintelligence” describes a subset of these activities, specifically, “information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities.” Examples of typical counterintelligence operations are the monitoring of foreign intelligence officers, the identification of possible espionage activities, the identification of international terrorist cells, and the monitoring, prevention, and disruption of terrorist activities. The distinguishing feature of a counterintelligence operation is that the target is a foreign power (state, quasi-state, or international terrorist group) or its agent; targets with no tie to a foreign power are not counterintelligence targets and typically are handled through criminal investigative channels.

Counterintelligence within the United States is primarily the responsibility of the FBI, which conducts counterintelligence operations under guidelines

13. Although the term “counterintelligence” encompasses operations targeting all types of foreign powers (both traditional state powers and international terrorist groups), many documents, and the organizational structure of some agencies, distinguish between two facets of counterintelligence, namely, operations against foreign states and their intelligence services as “counterintelligence” or “foreign counterintelligence,” and operations targeting international terrorist groups as “counterterrorism.” In this article I use “counterintelligence” to include both types of operations.
14. “Foreign power” and “agent of a foreign power” are key terms of art in counterintelligence. Definitions of both terms may be found in FISA at 50 U.S.C. §1801(a)-(b).
issued by the Attorney General. Counterintelligence operations occur outside the structure of the criminal law, although they may lead to criminal prosecutions for espionage or terrorism-related crimes.

Historically, counterintelligence operations were subject to very little oversight. The revelation of abuses by the FBI, CIA, and DOD during the 1960s and 1970s, however, prompted Congress to bring counterintelligence activities under a higher degree of regulation. The use of electronic surveillance in counterintelligence became subject to the Foreign Intelligence Surveillance Act of 1978 (FISA), which set boundaries on use of the technique and introduced judicial supervision. The same era saw the beginning of substantial executive branch regulation of U.S. counterintelligence and foreign intelligence activities.

One legacy of this period of regulation was an enduring concern that the tools available to counterintelligence should not be used to subvert the constitutional protections of the criminal law. This concern, which had its roots in pre-FISA case law, led to the creation of a “wall,” built of legal and policy requirements and reinforced by culture, that separated counterintelligence officers from criminal investigators. But the wall, prior to its partial dismantlement through the operation of the USA PATRIOT Act and a subsequent court decision, had the unintended consequence of depriving counterintelligence operators of some of the basic tools of criminal investigation.

---


18. The principal investigations of the abuses were conducted by the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the “Church Committee”) and the House Select Committee on Intelligence (the “Pike Committee”). See Richard A. Best, Jr., Proposals for Intelligence Reorganization 1949-2004 (Cong. Res. Serv. RL32500) (Jul. 29, 2004), at 17-25, available at http://www.fas.org/irp/crs/RL32500.pdf. See also Banks & Bowman, supra note 11, at 68-74.


21. See United States v. Truong Dinh Hung, 629 F.2d 908, 915-916 (4th Cir. 1980) (upholding a warrantless surveillance only so long as it was conducted “primarily” for foreign intelligence reasons).


23. In re Sealed Case, 310 F.3d 717 (Foreign Intelligence Surveillance Court of Review 2002).

24. There are many descriptions of the history and effects of the “wall” as it existed prior to the passage of the USA PATRIOT Act. See, e.g., id. at 721-728; Final Report of the Attorney General’s Review Team on the Handling of the Los Alamos National Laboratory Investigation, ch. 20 (May 2000), available at http://www.usdoj.gov/ag/readingroom/bellows20.pdf (commonly called the “Bellows Report,” this document examines the FBI investigation of Dr. Wen Ho Lee; Chapter 20 contains a detailed description of the “wall”); THE 9/11 COMMISSION
FBI counterintelligence agents were authorized by FISA to conduct electronic surveillance and physical searches. However, such methods are generally used only in the end stages of an investigation, after the probable cause required for FISA surveillance is established through the use of less intrusive techniques. Indeed, FBI counterintelligence agents are under a formal requirement to use the least intrusive means first. These less intrusive means include interviews, review of publicly available information, surveillance in areas where no reasonable expectation of privacy exists, consensual monitoring, “mail covers,” and the use of undercover operatives. They also include the use of “national security letters” to obtain information for counterintelligence purposes.

Congress approved the use of national security letters in response to the need for counterintelligence agents to obtain transactional information about investigative subjects. “Transactional” information broadly describes information that documents financial or communications transactions without necessarily revealing the substance of those transactions. Telephone billing records that list the numbers dialed by a particular subscriber, records from an Internet service provider showing when a user logged onto an account or to whom the user sent email, records of bank accounts or transfers of money between financial institutions, and credit records are all examples of transactional information.

Transactional information has developed into an extraordinarily valuable source of data for counterintelligence analysts, particularly in their efforts to identify international terrorists. Terrorists can limit their exposure to the interception of the content of communications by using counter-surveillance techniques that run the gamut from the ancient (human couriers, secret writing, simple word codes) to the modern (computer-based encryption and steganography). It is far more difficult for them to cover their transactional
footsteps. Therefore, counterintelligence analysts seek to use information about financial, credit, and communications transactions to construct link diagrams of terrorist networks. A good example of this technique is the extensive, and tragically retrospective, link analysis of the nineteen September 11 hijackers.

The legal status of transactional information has evolved dramatically since the mid-1970s, following public awareness that nearly all transactional information resides beyond the protections of the Fourth Amendment. In United States v. Miller, the Supreme Court held that the government can use a grand jury subpoena to obtain a defendant’s financial records from a bank without intruding into an area protected by the Fourth Amendment. The Court pointed out that “no interest legitimately protected by the Fourth Amendment” is implicated by governmental investigative activities unless there is an intrusion into a zone of privacy, into “the security a man relies upon when he places himself or his property within a constitutionally protected area.” The checks, deposit slips, and bank statements produced in response to the subpoena were not the defendant’s “private papers,” the Court held; rather, they contained “only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.” By handing over this information to a third party, the defendant took the risk that it would be conveyed to the government by that third party. Finally, the Court noted that the lack of notice to the defendant that the government had obtained his information did not infringe upon a protected interest.

To be sure, expectations of privacy may have changed in the three decades since Miller was decided. Commercial enterprises and financial institutions today commonly allow customers to state a preference about how their personal information will be used, and they often market guarantees of

---


32. Id. at 440, citing Hoffa v. United States, 385 U.S. 293, 301-302 (1966).
33. 425 U.S. at 440, 442.
34. Id. at 443.
35. Id. at 443 n.5; see also Securities and Exchange Comm’n v. Jerry T. O’Brien, Inc., 467 U.S. 735, 743 (1984).
privacy. From this, a customer now could reasonably conclude that he or she retained control over data entrusted to these third parties. In spite of criticism that it needs re-examination in light of these and other technological developments, however, Miller remains the law for now.

The Miller decision prompted Congress in 1978 to enact the Right to Financial Privacy Act (RFPA). In broad terms, the RFPA created statutory protection for the records that the Miller Court found were beyond the reach of the Fourth Amendment. The Act defined the scope of the records protected and generally required that notice be given to account holders when records were disclosed in response to legitimate government inquiries. The statute aimed to "strike a balance between customers’ right of privacy and the need of law enforcement agencies to obtain financial records pursuant to legitimate investigations." Congress included an exception for foreign intelligence investigations, allowing requests for protected information by government authorities who were "authorized to conduct foreign counter- or foreign positive-intelligence activities for purposes of conducting such activities" to be honored without notice to the targeted customers. Writing just two years after the Church and Pike Committees had completed their work, however, Congress remained wary of counterintelligence, and it noted that the exception should "be used only for legitimate foreign intelligence investigations; investigations proceeding only under the rubric of ‘national security’ do not qualify.'

By the mid-1980s, the FBI had begun to push for authority to compel the production of financial records in counterintelligence matters without a judicial order. The existing RFPA language allowed the FBI (and other counterintelligence agencies) to make requests for information, but it did not require financial institutions to comply. The FBI argued that while most such
institutions did comply, in “certain significant instances” they did not, often citing the constraints of state constitutions or banking privacy laws.\(^42\) The congressional response\(^43\) was to give the FBI\(^44\) specific authority to compel the production of financial records using a “national security letter.”\(^45\)

With the introduction of compulsory process, Congress also created safeguards to govern the FBI’s use of that authority. The statute required that a high-ranking FBI official certify: (1) that the information is sought “for foreign counterintelligence purposes,” and (2) that “there are specific and articulable facts giving reason to believe that the customer or entity whose records are sought is a foreign power or agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978.”\(^46\) The new provision, like the original RFPA, however, both failed to require notification of the target and affirmatively prohibited the financial institution from disclosing the existence of the national security letter to anyone.\(^47\) The House Permanent Select Committee on Intelligence found that the “FBI could not effectively monitor and counter the clandestine activities of hostile espionage agents and terrorists if they had to be notified that the FBI sought their financial records for a counterintelligence investigation.”\(^48\) Nevertheless, the legislators expressed a preference that the Director of the FBI restrict the delegation of national security letter authority and that the requirements for handling information obtained through the RFPA be integrated into the Attorney General’s guidelines for FBI counterintelligence.\(^49\)

Congress seemed far more receptive to the idea of FBI counterintelligence access to financial records in 1986 than it did in 1978. In part that could reflect a greater confidence in the regulation of counterintelligence activities. Executive Order 12,333\(^50\) was by that time firmly established as the basis for jurisdiction and operational rules within the U.S. intelligence community. Pursuant to that order, the FBI was operating under Attorney General guidelines that governed all counterintelligence activity and that set standards


\(^{44}\) Only the FBI has compulsory authority, although the request provision in 12 U.S.C. §3414(a)(1)(A) remains available to other agencies. The request provision is used, for example, by counterintelligence components within the Department of Defense. See Department of Defense Dir. No. 5400.12, Obtaining Information from Financial Institutions (Feb. 6, 1980), at encl. 5, available at http://www.dtic.mil/whs/directives/corres/html/540012.htm.

\(^{45}\) The term “national security letter” does not appear in the statute, but the legislative history indicates that it was in common use by that time. See H.R. Rep. No. 99-690(I), at 15.

\(^{46}\) Pub. L. No. 99-569, §404.

\(^{47}\) Id.


\(^{50}\) Exec. Order No. 12,333, supra note 12, at §3.4(a).
and approval authority for the various facets of counterintelligence investigations. The 1986 legislation may also reflect a change in attitude about the need for counterintelligence. The early 1980s saw a dramatic increase in espionage cases, and interest in counterintelligence rose accordingly. Moreover, Congress began to see international terrorism as a serious national security threat.

In granting compulsory process to FBI counterintelligence in 1986, Congress created a new, hybrid legal standard: “specific and articulable facts giving reason to believe” that the targeted person is an “agent of a foreign power.” The “agent of a foreign power” criterion was not new; it had been established in the Foreign Intelligence Surveillance Act of 1978 as a way to identify proper subjects of counterintelligence electronic surveillance. The

51. See FCI Guidelines, supra note 15.
55. FISA authorizes electronic surveillance (and, since 1994, physical searches) of foreign powers and their agents when the government demonstrates, inter alia, probable cause that the targets meet the relevant definitions. See generally 50 U.S.C. §§1801-1829. FISA defines “agent of a foreign power” as:

1. any person other than a United States person, who –
   (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;
   (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or

2. any person who –
   (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
   (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
   (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
   (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
   (E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to
innovation was in the quantum of proof required: “specific and articulable facts giving reason to believe.” The Conference Report noted that the standard was “significantly less stringent than the requirement of ‘probable cause,’” and it indicated that the “reason to believe” standard should “take into account the facts and circumstances that a prudent investigator would consider insofar as they provide an objective, factual basis for the determination.” An earlier report indicated that the House considered the higher standard of “probable cause” inappropriate, given the holding in *Miller*.

Shortly before Congress modified the RFPA to provide national security letter authority, it enacted the Electronic Communications Privacy Act (ECPA). ECPA broadly updated the law governing electronic communications by refining prohibitions on their interception, extending legal protections for traditional telephone service to include all wire and electronic communications services, and regulating stored wire and electronic communications.

In many respects, ECPA was an attempt to keep pace with evolving technology. It represented the first significant legislation to address what would become the Internet. In particular, ECPA was concerned with the invasive potential of advancing technology. The Senate report opened by quoting the prescient dissent in *Olmstead v. United States*: “Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.” The report continued by observing that the growing use of computers enabled the proliferation of personal information stored in areas beyond the control of the individual. Citing *Miller*, the report concluded that, absent statutory protection, such information “may be open to possible wrongful use and public disclosure by law enforcement authorities as well as unauthorized private parties.”

ECPA addressed this problem by extending statutory protection to electronic and wire communications stored by third parties (for example, on the servers of an Internet service provider or corporate network) and to

---

50 U.S.C. §1801(b).
60. See id.
61. Id. at 2, quoting *Olmstead v. United States*, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).
electronic communication transactional records.\footnote{53} The Act also restricted the government’s access to live telephone transactional data (commonly known as “pen register” and “trap and trace” data), requiring it to obtain a court order based upon a certification of relevance to an ongoing criminal investigation.\footnote{54}

Like the RFPA, ECPA contained a special provision for counterintelligence access. Section 201 of ECPA allowed the FBI to compel the production of “subscriber information and toll billing records information, or electronic communication transactional records” from a “wire or electronic communications service provider.”\footnote{65} The issuance of a national security letter under this provision required the certification of a high-ranking FBI official\footnote{66} that the information sought was relevant to a foreign counterintelligence investigation and that there were “specific and articulable facts giving reason to believe” that the target was a foreign power or agent of a foreign power under the FISA definitions.\footnote{67} The ECPA provision thus mirrored the standard in the 1986 amendment to the RFPA.

ECPA’s drafters also aimed for a “carefully balanced provision” that addressed operational necessities.\footnote{68} The “specific and articulable facts” standard emerged as an appropriate balance for counterintelligence access: criminal investigators could obtain information upon a certification of relevance (but generally with notice to the target), while counterintelligence investigators could obtain the information in secret,\footnote{69} but only after meeting...
the more stringent standard. The standard was viewed as consistent with the investigative standards imposed on FBI counterintelligence by the Attorney General guidelines.70

The counterintelligence provision of ECPA was amended twice prior to the passage of the USA PATRIOT Act. It originally gave the FBI access to subscriber information, toll billing records, and electronic communications transactional records of anyone who met the FISA definition of a foreign power or agent of a foreign power (to the “specific and articulable facts” standard).71 The FBI subsequently sought authority to obtain subscriber information in order to identify (or to confirm the identity of) people who contacted or were in contact with agents of a foreign power.72 The FBI offered three operational examples: (1) persons whose phone numbers were listed in an address book seized from a suspected terrorist; (2) persons who called a foreign embassy and asked to speak to an intelligence officer; and (3) callers to the home of a suspected intelligence officer or terrorist.73 In each case, the FBI’s use of ECPA’s counterintelligence provision or other authorities against a foreign intelligence officer or terrorist target would yield the phone number of the caller, but the FBI could not obtain subscriber information about that caller. A 1993 amendment to ECPA gave the FBI the authority it sought, with some limitations.74 Congress amended the provision again in 1997, expressly

70. The portions of the Attorney General guidelines setting out the standards for opening the various forms of counterintelligence investigations remain classified. ECPA’s legislative history notes cryptically that “the Senate Select Committee on Intelligence has informed the Judiciary Committee that the language contained in the bill would not significantly alter the application of the current FBI investigative standard in this area.” S. REP. NO. 99-541, at 45.


73. Id. at 3.

74. The new language gave the FBI access to subscriber information on anyone who was in contact with a terrorist, but it limited that access to situations in which circumstances “gave reason to believe that the communication concerned” terrorism or clandestine intelligence activities. See Act of Nov. 17, 1993, Pub. L. No. 103-142, §2, 107 Stat. 1491, 1492 (1993). This distinction was meant to clarify that the authority not be used to target innocent contacts with agents of foreign powers, such as routine calls to foreign embassy staff about visas or other general information matters. See H.R. REP. NO. 103-46, at 2-3.
defining the phrase “toll billing records” to mean “local and long distance toll
billing records.”

The final type of national security letter emerged in 1995, when the FBI
sought counterintelligence access to credit records. The FBI stated that
RFPA national security letters had proven very useful, but that counter-
intelligence agents still had to employ intrusive or time-consuming techniques
(physical and electronic surveillance, mail covers, and canvassing of local
banks) simply to determine where targeted individuals maintained accounts.
The same information was readily available from credit bureaus (“consumer
reporting agencies”) and was commonly obtained in criminal investigations
through the use of a subpoena. Congress’s response was to amend the Fair
Credit Reporting Act (FCRA) by giving the FBI national security letter
authority to obtain certain information from credit reporting agencies. The
authority essentially replicated that granted in the 1993 ECPA amendment,
employing the same legal standard: “necessary for the conduct of an
authorized foreign counterintelligence investigation” and “specific and
articulable facts” giving reason to believe the target was (or was in contact
with) an agent of a foreign power. Similarly, the new FCRA provision
embodied two levels of access to information: if the target was an agent of a
foreign power, the FBI could get the identity of all financial institutions at
which the target maintained an account; if the target was merely in contact
with an agent of a foreign power, the FBI got “identifying information”
limited to “name, address, former addresses, places of employment, or former
places of employment.”

The one departure from the RFPA and ECPA models was in the area of
disclosure. The FCRA language prohibits disclosure of the national security
letter by employees of the credit reporting agency “other than [to] those
officers, employees, or agents of a consumer reporting agency necessary to
fulfill the requirement to disclose information” to the FBI. This language
was intended to clarify what is apparently assumed in the other statutes,
namely, that employees may disclose the existence of the national security

---

983, 996-998.
77. See id. at 36.
78. See id. at 35-36.
2002)).
82. Id.
83. Id. The ECPA and RFPA provisions prohibit disclosure to “any person.” 18 U.S.C.
§2709(c) (ECPA); 12 U.S.C. §3414(a)(5)(D) (RFPA).
letter in compliance with the credit bureau’s internal policies.\textsuperscript{84} Presumably, this language would permit disclosure to relevant managers or the consumer reporting agency’s legal counsel. Finally, the FCRA amendment gave the FBI access to a consumer’s full credit report, but only if a court found that the FBI’s information met the same legal standard – “specific and articulable facts” – as in the other section of the amendment.\textsuperscript{85}

In addition to the national security letter authorities just described, in a 1998 amendment to the Foreign Intelligence Surveillance Act the FBI acquired two new tools to collect transactional information.\textsuperscript{86} The amendment for the first time permitted “pen register” and “trap and trace” authorization to be obtained through the FISA process.\textsuperscript{87} This change addressed a longstanding anomaly in the counterintelligence environment: unlike criminal investigators who could use Title 18 authority to install pen registers and trap and trace devices,\textsuperscript{88} counterintelligence agents could not prospectively collect telephone transactional information on suspected spies or terrorists.\textsuperscript{89} The new FISA pen register and trap and trace authority mirrored the criminal investigative authority that had existed since 1986.\textsuperscript{90} Unlike the criminal statute, however, the standard for a FISA pen register or trap and trace order was not “relevance” to an ongoing investigation. Rather, it was set at something like the hybrid standard for national security letters: “relevance” plus “information which demonstrates that there is reason to believe” that the targeted telephone line “has been or is about to be used in communication with” a person engaged in international terrorism, a person engaged in clandestine intelligence activities, or any foreign power or agent of a foreign power under circumstances indicating clandestine intelligence or terrorist

\textsuperscript{84} See H.R. CONF. REP. NO. 104-427, at 39; see also Doe v. Ashcroft, supra note 69, at 51-55 (comparing non-disclosure language in FCRA to that in ECPA).

\textsuperscript{85} Pub. L. No. 104-93, §601(a). The provision was largely useless prior to the USA PATRIOT Act, since FBI counterintelligence agents did not have ready access to a court that could issue such an order. The Foreign Intelligence Surveillance Court likely had no jurisdiction to entertain a request under this section. See 50 U.S.C. §§1803(a), 1822(c) (defining jurisdiction of the court). Recourse to a federal district court would have involved interaction with prosecutors, and thus triggered elaborate “wall” restrictions meant to keep counterintelligence agents and prosecutors at arm’s length. See supra note 24. Obtaining a simple credit report typically would not have justified the efforts and risks associated with those restrictions.


\textsuperscript{87} Id. at §601, 112 Stat. 2396, 2404-2410.

\textsuperscript{88} See 18 U.S.C. §§3121-3127.

\textsuperscript{89} Counterintelligence agents could, however, collect historical transactional data using the ECPA national security letter authority. See 18 U.S.C.§2709.

\textsuperscript{90} See generally Pub. L. No. 105-272, at §601, 112 Stat. 2396, 2404-2410. The analogous criminal law authority is codified at 18 U.S.C. §§3121-3127 and authorizes the use of pen registers and trap and trace devices upon a government certification that the information likely to be obtained is relevant to an ongoing criminal investigation. Id. at §3123(a).
activities. The FISA amendment also created procedures for emergency use of the authority, certain restrictions on the use of information obtained through the authority, and a notification and challenge procedure triggered when information obtained is used in a subsequent proceeding. The notification and challenge procedure mirrors those found elsewhere in FISA for electronic surveillance and physical searches.

The 1998 amendment to FISA also created the direct antecedent of §215 of the USA PATRIOT Act. It allowed the FBI to seek a FISA court order compelling the production of business records from common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities. The standard was set at the now-familiar “specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or agent of a foreign power.” Like the new pen register authority and all of the existing national security letter authorities, this provision imposed a non-disclosure requirement on the recipients of the court order. In stating the duties of the Foreign Intelligence Surveillance Court judge, it simply replicated the language of the pen register and trap and trace provision: “Upon application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified . . . if the judge finds that the application satisfies the requirements of this section.”

There is almost no legislative history for these two new provisions. They emerged in the Senate version of the Intelligence Authorization Act for Fiscal Year 1999, but they are not otherwise mentioned in the conference report or floor debate. The congressional debate and the press tended to focus on another section, which amended the criminal electronic surveillance law (commonly called “Title III”) to facilitate “roving” surveillance. It is reasonable to assume that, as in prior instances, the FBI argued that it needed authority to compel production of materials not then accessible through the use of national security letters. Since counterintelligence agents were

95. Id.
96. Id. The non-disclosure provision incorporated the clarifying language (“other than those officers, agents or employees . . . necessary to fulfill the requirement”) developed for the FCRA national security letter. Id.; see supra text accompanying notes 83-84.
99. Pub. L. No. 105-272, §604, 112 Stat. 2396, 2413; see, e.g., Vernon Loeb, Anti-Terrorism Powers Grow, “Roving” Wiretaps, Secret Court Orders Used to Hunt Suspects, WASH. POST, Jan. 29, 1999, at A23. The fact that the change to Title III (a criminal authority) occurred via the intelligence authorization act was particularly controversial and dominated the public debate.
“walled” off from the use of criminal authorities like grand jury subpoenas, a
records custodian could effectively stall a counterintelligence investigation by
refusing to release records absent compulsory process.106 Such a refusal could
have been motivated by a concern over the effect of state laws or civil
liability, or it could have been an act of civil disobedience or simple
unwillingness to cooperate.101

In summary, on the eve of the September 11 terrorist attacks the FBI had
five separate legal authorities that addressed the need to compel production of
transactional information in counterintelligence investigations: three types of
national security letters (under RFPA, ECPA, and FCRA),102 the FISA pen
register/trap and trace authority, and the FISA business records authority. All
of these authorities specified the types of records that could be obtained, and
all the records specified were, according to the reasoning of the Supreme
Court in Miller, outside the protection of the Fourth Amendment. All of the
authorities required, in essence, that the information sought be relevant to an
authorized counterintelligence investigation and that the FBI demonstrate
“specific and articulable facts giving reason to believe” that the investigative
targets were foreign powers or agents thereof.

II. THE USA PATRIOT ACT AND SECTION 215

Much has already been written about the creation of the USA PATRIOT
Act in the chaotic weeks following September 11, 2001.103 The Bush
administration began developing a legislative proposal within days after the attacks. Congress acted with great speed: the House version of the Act was introduced on October 2 and passed ten days later; the Senate version was introduced on October 4 and passed in just seven days. The final version of the Act was introduced on October 23, 2001, and was signed into law on October 26, 2001. The end product is massive, running to 130 printed pages.

A very considerable portion of the Act is devoted to changes in criminal, immigration, and money laundering statutes. Within the sections that affect counterintelligence authorities, the revisions to national security letter and related authorities are generally overshadowed by enhancements to the FISA search and surveillance provisions and new rules for information sharing.

The USA PATRIOT Act revisions to authorities governing counterintelligence access to transactional information are spread across three sections: §214 (“Pen register and trap and trace authority under FISA”), §215 (“Access to records and other items under the Foreign Intelligence Surveillance Act”), and §505 (“Miscellaneous national security authorities”). The cumulative effect of these three sections is to make an across-the-board adjustment of the legal standard for access from “relevance” plus “specific and articulable facts giving reason to believe” the target was a foreign power or an agent of one, to simple “relevance” to an investigation to protect against international terrorism or clandestine intelligence activities (provided such an investigation of a U.S. person is not based solely on protected First

---


109. See id.
Section 505 also lowers the signature authority for the three types of FBI national security letters from Deputy Assistant Director to Special Agent in Charge. The apparent intent of Congress here was to make the legal standard for basic counterintelligence investigations analogous to that for the corresponding criminal investigations, a change viewed as appropriate in light of the evolving terrorist threat. In a different section, the Act creates a broad new investigative authority by inserting language in the FCRA that compels consumer reporting agencies to furnish a consumer report of a consumer and all other information in a consumer’s file to a government agency authorized to conduct investigations of, intelligence or counterintelligence activities or analysis related to, international terrorism when presented with a
written certification by such government agency that such information is necessary for the agency’s conduct of such investigation, activity, or analysis.\textsuperscript{113}

Of the various revisions, those in §215 go farthest. Like the other counterintelligence authorities for transactional information, §215 incorporates the new “relevance” standard, but it lacks language limiting its application to specific types of records. Section 215 replaces the old “business records” authority in Title V of FISA with new language (italics indicate changes made by the USA PATRIOT Act):\textsuperscript{114}

\section*{§1861. Access to certain business records for foreign intelligence and international terrorism investigations}

(a) (1) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application 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, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

(2) An investigation conducted under this section shall –

(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and

(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

\begin{footnotesize}
\begin{enumerate}
\item See 15 U.S.C. §1681v. This extraordinary provision, which has attracted surprisingly little notice, was buried in the money laundering provisions of Title III of the Act. See Pub. L. No. 107-56, §358(g)(1)(B), 115 Stat. 272, 327-328 (2001). Unlike other national security letters, the authority is limited to international terrorism matters, but it extends to agencies other than the FBI. The language of the provision and its position in the Act suggest that it was developed in isolation from the other changes to counterintelligence authorities. The new authority, for example, is not noted in the FBI’s initial summary of the USA PATRIOT Act changes. See supra note 100.
\item Unless otherwise noted, citations to USA PATRIOT Act §215 hereinafter are to its provisions as codified in the U.S. Code.
\end{enumerate}
\end{footnotesize}
(b) Each application under this section—

(1) shall be made to—

(A) a judge of the court established by section 103(a); or

(B) a United States Magistrate Judge under chapter 43 of title 28, United States Code, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and

(2) shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

(c) (1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section.

(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a).

(d) No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section.

(e) A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

While the old language allowed the FBI to seek “an order authorizing a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility to release records in its possession,” the new section allows an order requiring the production of “any tangible things (including books, records, papers, documents, and other items)” The new language, like the new national security letter language, includes the caveat that the material sought 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, provided that such investigation of a United States person is not conducted solely upon the basis

of activities protected by the first amendment to the Constitution.”  A new paragraph curiously repeats the First Amendment constraint from the preceding paragraph. The old standard that there be “specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or agent of a foreign power” is replaced by a specification that the records sought be for an “authorized investigation,” as defined in an earlier paragraph. There are no changes to the role of the court (“the judge shall enter an ex parte order as requested”), and the changes to the non-disclosure language simply recognize the broader scope of the records sought. Section 215 adds a “good faith” defense against civil liability for those who comply with the orders, and it specifies that production shall not be deemed a waiver of privileges in other proceedings or contexts.

Unfortunately, there is very little in the way of legislative history for §215. The provision appeared in the House version of the USA PATRIOT Act, but its substance is discussed neither in the House report nor in any floor debate. The one fact that emerges from the House materials is that §215 was a substitute for “administrative subpoena” authority that the government had originally sought. The Senate record is even less illuminating, consisting only of transcripts of two floor debates. However, the Senate debated an amendment to §215 offered by Senator Feingold which, though defeated, raised key criticisms that served to shape the subsequent public debate.

Public criticism of the USA PATRIOT Act began almost immediately, with expressions of concern over the speed with which the legislation was produced and the lack of public hearings. Some members of Congress suggested that the Administration, and particularly the Attorney General, were exploiting the chaotic post-9/11 environment to accomplish a dramatic expansion of executive branch authority. Although criticism of the Act in general, and of §215 in particular, has proliferated since passage, the key issues remain those first identified in the Senate debates surrounding the

117. Id.
118. Id. §1861(a)(2).
119. Id. §1861(b)(2).
120. Id. §1861(c)-(d).
121. Id. §1861(e).
122. Id. §1862.
125. See H.R. REP. No. 107-236 (Part I), at 61.
126. A debate on October 11, 2001, addressed the Senate version of the Act (S. 1510). 147 CONG. REC. S10,547-S10,630. Another on October 25, 2001, considered the final version of the Act (H.R. 3162). 147 CONG. REC. S10,990-S11,059.
Feingold amendment. There are three general criticisms: (1) §215 violates the Fourth Amendment and/or various statutory protections because it allows the government to compel production of personal information without a showing of probable cause; (2) §215 is impermissibly broad, in that it allows the FBI access to information about innocent third parties upon a showing of mere relevance to an investigation; and (3) there is no effective oversight of the use of §215.

The broad scope of the “any tangible things” language prompted charges that the section violates the Fourth Amendment by “not requir[ing] the government to get a warrant or establish probable cause” before it demands “personal records or belongings” and by failing to satisfy the notice requirements of the Fourth Amendment. In somewhat more muted terms, Senator Feingold emphasized the way the provision overrides state and federal laws that protect records “containing sensitive personal information such as medical records from hospitals or doctors, or educational records, or records of what books somebody has taken out of the library.” Library records have emerged as the most controversial example of “tangible things” covered by §215, especially since government access to them seems to raise state law, First Amendment, and Fourth Amendment issues.

Library and bookseller associations are probably now the most aggressive opponents of §215, with the libraries motivated, in part, by their historical experience with FBI counterintelligence operations. Not all of their legal arguments withstand a closer look, however. For example, the

---

130. See 147 CONG. REC. S10,583-S10,586 (2001) (debate on Sen. Feingold’s proposed amendment to §215). After his amendment was rejected, Senator Feingold reiterated his concerns during the final Senate debate on the Act. See 147 CONG. REC. S11,019-S11,023 (2001). Senator Feingold was the only member of the Senate to vote against passage of the USA PATRIOT Act. Reports prepared by the American Civil Liberties Union subsequent to the passage of the Act incorporate and expand upon Senator Feingold’s criticisms of §215. See Beeson & Jaffer, supra note 3.

131. See Beeson & Jaffer, supra note 3, at 7.

132. See 147 CONG. REC. S10,583-S10,584 (2001).


134. During the Cold War, the FBI established a counterintelligence program known as the “Library Awareness Program.” FBI agents visited libraries (particularly technical and academic libraries) for the purpose of monitoring foreign intelligence officers who were exploiting open source information from library collections. FBI counterintelligence agents attempted to recruit library staff to monitor and report on “suspicious” activities by library patrons. FBI agents also sought library circulation records and other materials. When the program came to light, there was widespread opposition to it. Litigation and congressional inquiries followed and persisted into the 1980s. Despite several attempts to craft legislation to address the issues raised by this episode, Congress never enacted a federal statute protecting library records. See generally HERBERT N. FOERSTEL, SURVEILLANCE IN THE STACKS: THE FBI’S LIBRARY AWARENESS PROGRAM (1991).
claim that library patron records are protected by the Fourth Amendment is not convincing, even to sympathetic commentators. Rather, library patron records fall squarely into the category identified in United States v. Miller, that is, information that ceases to be a person’s “private papers” by virtue of its being handed over to a third party who may convey it to the government. The Justice Department certainly espoused this view, arguing that “[a]ny right of privacy possessed by library and bookstore patrons in such information is necessarily and inherently limited since, by the nature of these transactions, the patron is reposing that information in the library or bookstore and assumes the risk that the entity may disclose it to another.” Indeed, this same view was expressed in the congressional debate on the USA PATRIOT Act.

The controversy over library records might not be nearly so acrimonious if the First and Fourth Amendment issues could be addressed by separating the names of borrowers from the titles (and by inference from the contents) of the books they borrow. Such “anonymization” of personal reading habits might be required if §215 provided access only to purely transactional information. Thus, information that would identify a library borrower, such as name and address, would be held strictly apart from a book’s title. Only if intelligence analysts subsequently linked either the book or the borrower to a credible threat would the two kinds of data be re-associated, perhaps with the approval of a neutral magistrate. Given that §215 was clearly part of a set of parallel revisions to all FBI counterintelligence authorities for access to transactional information (national security letters, pen register/trap and trace, and business records), it seems reasonable to conclude that Congress saw §215 as applying only to transactional information that is not subject to constitutional protections. The limitation of §215 to transactional records also would be consistent with the historical development of FBI counterintelligence authorities sketched out in Part I.

Whatever the intention of Congress or the understanding of the executive branch, however, there is no indication in the language of §215 that it is so limited. The lack of clarity about this point has created significant confusion. The FBI, for example, notes the uncertain scope of §215 (and the problem of library records) in its legal instructions to FBI agents on the use of §215 authority. In this respect, §215 parts company with the other “transactional” counterintelligence authorities, all of which specify the data to which they apply.

135. See Klinefelter, supra note 133, at 225-226. But see Martin, supra note 133.
138. See 147 CONG. REC. S10,993 (2001) (comments of Sen. Leahy) (the Fourth Amendment “does not normally apply” to techniques such as the FISA pen register and access to records authority).
apply, either explicitly or by their incorporation into the very statutes that protect the information at issue. ¹⁴⁰

How did this departure from the established pattern of clear limitation to transactional information occur? I suggest that a clue is to be found in Congress’s rejection of the Administration’s proposal for “administrative subpoena” authority to obtain business records. ¹⁴¹ Congress rejected that proposal in favor of the § 215 language, apparently concluding that the requirement of a court order in § 215 was more protective of privacy interests. ¹⁴² In the process it may have felt that the involvement of a neutral magistrate made a limitation on the type of information less important. There are, however, some hints in the text of § 215 that elements of the “administrative subpoena” proposal were simply inserted into the existing FISA business records provision. For example, the phrase “production of any tangible things (including books, records, papers, documents, and other items)” ¹⁴³ closely tracks language in the Attorney General’s administrative subpoena authority for use in drug investigations, which requires “production of any records (including books, papers, documents, and other tangible things).” ¹⁴⁴ If so, Congress might have thought it was prescribing the kind of limited scope found in the administrative subpoena authorities.

Whatever the provenance of the § 215 text, abandonment of the administrative subpoena option foreclosed one proven path to securing constitutionally permissible access. Administrative subpoenas have long been available to executive branch agencies, and they now exist in at least 335


¹⁴¹ The text of the Administration’s legislative proposals is not publicly available, but it is described by various references in the legislative history and congressional debates. See, e.g., H.R. Rep. No. 107-236 (Part I), at 61. In addition, a “Consultation Draft” containing a version of the Administration’s proposal appears in materials prepared by the House Judiciary Committee. See Administration’s Draft Anti-Terrorism Act of 2001, supra note 111, at 45-90. The Consultation Draft includes a proposed amendment to FISA that would have replaced the old business records authority with language allowing the Attorney General to require the production of any tangible things “by administrative subpoena.” Id. at 74.


¹⁴⁴ 21 U.S.C. § 876(a). Section 876 subpoenas are commonly used by the DEA and FBI, and they would serve as a logical model for a counterintelligence administrative subpoena. In the Consultation Draft prepared for the House Judiciary Committee, § 876 is identified as the “model” for the Administration’s business records proposal, although the draft language provided is less detailed than that found in § 876. See Administration’s Draft Anti-Terrorism Act of 2001, supra note 111, at 57, 74. Following enactment of the USA PATRIOT Act, a bill creating an administrative subpoena in terrorism matters (modeled explicitly on 21 U.S.C. § 876) was introduced in the House but not passed. See Antiterrorism Tools Enhancements Act of 2003, H.R. 3037, 108th Cong., § 3.
There is a substantial body of case law approving the use of administrative subpoenas, including Supreme Court decisions establishing general standards. A key feature of administrative subpoena authority is its bifurcation of the authority to issue (held by the agency) and the authority to enforce (held by a court). This arrangement may facilitate testing the proper scope of a particular subpoena authority in court (provided the target whose records are obtained is given notice), especially if the authority is applied in a novel or controversial context. Despite the diversity of administrative subpoena authorities, moreover, the distinct enforcement role of the courts, coupled with internal agency guidelines on subpoena use, dissemination of information, and compliance with other privacy or notice requirements, are effective mechanisms to police the use of administrative subpoena authority.

Unlike authorities for administrative subpoenas, national security letter authorities do not include explicit enforcement mechanisms. If the recipient of a national security letter refuses to comply, the government must approach a federal court for enforcement. There are no reported decisions indicating that this has occurred, but if it did happen, the court could draw on existing administrative subpoena case law to resolve questions of scope and proper use.

147. See Report to Congress on the Use of Administrative Subpoena Authorities, supra note 145, at 7-14.
148. See id.; see also, e.g., In re Sealed Case (Administrative Subpoena), 42 F.3d 1412 (D.C. Cir. 1994) (discussing the limits placed on an administrative subpoena by relevance and investigatory purpose).
149. See Report to Congress on the Use of Administrative Subpoena Authorities, supra note 145, at 5, 9-25 (discussing standards for enforcement, dissemination, and notice relevant to various administrative subpoena authorities).
151. But cf. Doe v. Ashcroft, supra note 69, at 47-51 (discussing the absence of a clear enforcement mechanism for national security letters). Despite the counterintelligence context, the FBI could not seek the aid of the Foreign Intelligence Surveillance Court, since that court’s jurisdiction is limited to considering applications made pursuant to the FISA. See 50 U.S.C. §§1803(a), 1822(c).
152. There are several factors that may explain the lack of national security letter enforcement cases. Since the national security letter authorities specify the data to which they apply, and since they are directed to entities accustomed to receiving legal process (financial institutions, credit bureaus, communications providers), there may have been little occasion for controversy over the scope or application of the authority. It could also be the case that the FBI simply does not pursue enforcement in order to avoid any risk of compromising ongoing counterintelligence operations through litigation in federal courts. This situation could change as national security letter authorities are applied to a wider range of entities. See Intelligence
In contrast to the administrative subpoena authority sought by the Administration, the language of §215 seems to rule out an easy test of its scope. Under §215 a records custodian immediately receives a FISA Court order to provide government access to “tangible things,” so failure to comply does not trigger an enforcement proceeding, but instead places the recipient in peril of being held in contempt.153

The second major criticism of §215 concerns the movement from the standard of “specific and articulable facts giving reason to believe” that the target is an agent of a foreign power to a standard of “relevance to an authorized investigation to protect against international terrorism or clandestine intelligence activities.”154 Critics charge that this change gives the FBI too much authority, allowing the Bureau to conduct “fishing expeditions” by seeking the records of people who are not actual targets of an investigation.155 Some of these critics illustrate their point with hypotheticals based on imagined applications of the section.156

It is undeniable, of course, that the USA PATRIOT Act lowered the standards for counterintelligence collections. This change was carefully considered, however, and it apparently was influenced by the FBI’s supply of examples from actual operations. Even Senator Patrick Leahy, who is generally suspicious of expanded FBI authorities,157 found that the “FBI has made a clear case that a relevance standard is appropriate for counterintelligence and counterterrorism investigations, as well as for criminal investigations.”158 Other members echoed the idea that counterintelligence agents pursuing terrorists should have tools at least as readily available as those open to criminal investigators.159

There are two additional considerations relevant to this criticism. First, the more strident critics assume that the government, in the interest of

Authorization Act for Fiscal Year 2004, Pub. L. No. 108-177, §374, 117 Stat. 2599, 2628 (2003) (expanding the definition of “financial institutions” to which the RFPA national security letter authority applies). While it is not an enforcement case per se, Doe v. Ashcroft, supra note 69, contains a lengthy discussion of issues surrounding the enforcement of national security letters. Id. at 45-83. The holding that ECPA national security letters are unconstitutional rests, in part, on the lack of any clear procedural protections or review mechanism for this authority. Id. at 118-119.

153. The court would have the power to punish the contempt pursuant to 18 U.S.C. §401 (2000 & Supp. II 2002). Concerning the possibility of civil disobedience, see Klinefelter, supra note 133, at 226.
155. See Beeson & Jaffer, supra note 3, at 1-3; see also 147 CONG. REC. S10,583-S10,584, S11,022 (2001) (comments of Sen. Feingold).
156. See, e.g., Beeson & Jaffer, supra note 3, at 1.
157. Senator Leahy prefaced his introduction of the USA PATRIOT Act with a lengthy recitation of counterintelligence abuses dating back to the 1960s and 1970s, 147 CONG. REC. S10,992-S10,994 (2001), and he referred at one point to J. Edgar Hoover’s “totalitarian control” of the FBI. 147 CONG. REC. S11,015 (2001).
158. 147 CONG. REC. S10,557 (2001).
159. See supra note 112.
unjustified “fishing expeditions,” would be willing to collect information on innocent people not truly “relevant” to any authorized investigation.\textsuperscript{160} If this were true, however, the pre-USA PATRIOT Act standard offered no greater protection. The old version of the FISA business records authority did not require the court to find that there were “specific and articulable” facts; the government simply had to present a certification that “specific and articulable” facts existed.\textsuperscript{161} Unlike a FISA court judge considering an application for an electronic surveillance or physical search, the judge considering a business records application was not required to examine the facts supporting the government’s certification.\textsuperscript{162} For counterintelligence access to transactional information, both before and after the USA PATRIOT Act, the determination of whether the legal standard (“specific and articulable facts” before the Act, or “relevance” after) has been met rests solely with the FBI.

Second, the permissiveness of the new “relevance” standard in allowing the collection of information about persons who are not the targets of investigations is not necessarily a dramatic departure from the pre-USA PATRIOT Act environment. The FCRA and ECPA national security letters,\textsuperscript{163} as well as the FISA pen register/trap and trace authority,\textsuperscript{164} allowed some collection on persons who were merely in communication with targets that met the “specific and articulable” standard. The relevance standard does, of course, broaden the scope of the collection (and the persons subject to it),\textsuperscript{165} but its adoption is consistent with the general intention to make counterintelligence authorities comparable to criminal investigative ones.

It may be argued that the value of pre-USA PATRIOT Act authorities as investigative tools was unduly limited by the constraints on their availability. A clear goal of counterintelligence is to identify spies and international terrorists. If an investigator has specific and articulable facts that a target is an international terrorist, she has already achieved that goal. The authorities that incorporated the “specific and articulable” standard were useful to help

\begin{itemize}
  \item \textsuperscript{160} See Beeson & Jaffer, \textit{supra} note 3, at 1.
  \item \textsuperscript{161} Pub. L. No. 105-272, §602.
  \item \textsuperscript{162} \textit{Compare} 50 U.S.C. §§1805(a), 1824(a) (judge shall enter an order authorizing electronic surveillance or physical search if the judge finds that the relevant factual standards have been met) \textit{with} Pub. L. No. 105-272, §602 (judge shall enter an order if the FBI application contains the required certification that “specific and articulable facts” exist).
  \item \textsuperscript{163} Pub. L. No. 104-93, §601, 109 Stat. 961, 974-975 (1996) (authorizing use of FCRA national security letter to collect information on person who “has been, or is about to be, in contact with a foreign power or an agent of a foreign power”); Pub. L. No. 103-142, §1, 107 Stat. 1491, 1491-1492 (1993) (authorizing use of ECPA national security letters to collect information on certain persons “in communication with” a foreign power or an agent of a foreign power).
  \item \textsuperscript{164} See Pub. L. No. 105-272, §601, 112 Stat. 2396, 2406 (1998) (authorizing collection of pen register/trap and trace data on a communication instrument that “has been used or is about to be used in communication with” a foreign power or agent of a foreign power).
  \item \textsuperscript{165} The new standard apparently would allow collection on persons who were relevant to the investigation but who were not necessarily in communication with the agent of a foreign power.
\end{itemize}
build “probable cause” to conduct a search or electronic surveillance of an identified target, but they did not help in the perhaps more pressing task of sorting through the target’s associates to determine whether others were involved in the terrorist activity. Criminal investigators also perform this task, but they have access to compulsory legal process (grand jury or administrative subpoenas) to obtain relevant investigative information.\(^{166}\) While it may appear that counterintelligence agents operated successfully under such conditions for the twenty years prior to the USA PATRIOT Act, there is a growing consensus that, whatever the FBI’s capacity to deal with traditional intelligence and espionage threats, it was not properly equipped to meet the counterterrorism challenges of the late 1990s.\(^{167}\)

The third major criticism of §215 is that it lacks effective oversight for the exercise of such an expansive power, in the form of judicial approval, executive branch or congressional review, or notice to surveillance targets. Critics claim that although exercise of the power requires a court order, the judge has no meaningful discretion in considering a §215 application. While the plain language of §215 directs the judge to issue the business records order if the judge finds “that the application meets the requirements” of the section,\(^{168}\) the only “requirement” (aside from making the application to a FISA judge or a specially designated magistrate)\(^{169}\) is that the application specify that “the records concerned are sought for an authorized investigation.”\(^{170}\) The language describing the judge’s role is essentially the same as that found in FISA’s pen register/trap and trace provisions (both the pre- and post-USA PATRIOT Act versions),\(^{171}\) which appear to be derived from the criminal pen register statute.\(^{172}\) The Justice Department has made statements implying that the court does exercise some discretion, but it points to no support for this proposition.\(^{173}\) In the context of criminal pen registers, the United States Court of Appeals for the Tenth Circuit has found that the limited judicial review of a pen register request does not render the statute

\(^{166}\) The standard for a grand jury subpoena is not probable cause but relevance to a criminal investigation. Moreover, the relevance standard applied in the context of grand jury subpoenas is very broad. See United States v. R. Enterprises, Inc., 498 U.S. 292, 301 (1991) (subpoenas are not irrelevant if there is any reasonable possibility that they will produce information relevant to the general subject of the investigation).

\(^{167}\) See THE 9/11 COMMISSION REPORT, supra note 24, at 263-277, 350-360.

\(^{168}\) 50 U.S.C. §1861(c)(1).

\(^{169}\) Id. §1861(b)(1). There is no indication that the Chief Justice has ever designated a magistrate as permitted by §1861(b)(1)(B).

\(^{170}\) Id. §1861(b)(2).

\(^{171}\) Id. §1842(d)(1).

\(^{172}\) 18 U.S.C. §3123(a).

\(^{173}\) See Letter from Assistant Attorney General Bryant to Senator Leahy (Dec. 23, 2002), encl. at 3, available at http://fas.org/irp/agency/doi/fisa/doi-fisa-patriot-122302.pdf (“The FISA Court will not order the production of business records unless it can be shown that the individual for whom the records are being sought is related to an authorized investigation.”) (emphasis in original).
unconstitutional.  The Court recognized, but did not decide, the question of whether, despite the language of the statute, the reviewing court could inquire into “the government’s factual basis for believing” that the request is relevant.  The criticism of §215 on this point remains valid: the practical nature of the FISA court judge’s review of a business records application remains uncertain, as does the propriety of the standard of review, in light of the broad scope of §215 authority.

The oversight criticism also manifests itself in concern over what constitutes an “investigation.” Some commentators imply that the FBI can initiate investigations at will and that it can use such investigations as a pretext to “go fishing” in the great pool of personal information.  Such criticisms often ignore, or discount the effect of, the regulations applicable to counterintelligence activities. The FBI is only authorized to conduct counterintelligence in compliance with regulations established by the Attorney General.  Those regulations, in the form of guidelines, limit the subject matter of investigations, set standards for the various levels of investigation, and require that investigations be conducted in accordance with the Constitution and the laws of the United States.  The guidelines also require extensive reporting of FBI counterintelligence activities to oversight components within the Justice Department.  By executive order, the FBI and Justice Department also must report to the Intelligence Oversight Board, which has the authority to review intelligence activities and guidelines.

174. United States v. Hallmark, 911 F.2d 399, 402 (10th Cir. 1990). The decision rested, at least in part, on the holding that pen register data are not subject to Fourth Amendment protection.  See id., citing Smith v. Maryland, 442 U.S. 735, 739-746 (1979).
175. Hallmark, 911 F.2d at 402 n.3.
176. See supra note 155.
177. Exec. Order No. 12,333, supra note 12, at §1.14
178. See NSI Guidelines, supra note 17, at 6-7 (authorizing investigations to protect against defined threats to the national security).
179. See id. at 3. The Guidelines authorize three levels of investigative activity: threat assessments, preliminary investigations, and full investigations. The specific standards for initiating each level of investigation remain classified. See id. at 11-17.
180. The Guidelines provide in part:
These Guidelines do not authorize investigating or maintaining information on United States persons solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States. Rather, all activities under these Guidelines must have a valid purpose consistent with these Guidelines, and must be carried out in conformity with the Constitution and all applicable statutes, executive orders, Department of Justice regulations and policies, and Attorney General guidelines.
Id. at 7-8.
181. See id. at 14 (reporting of preliminary and full investigations), 17 (periodic summaries of full investigations), 25-27 (reporting of all information relevant to national security threats or crimes).
182. Executive Order No. 12,863 requires the reporting of intelligence activities that violate any executive orders or presidential directives to the Intelligence Oversight Board, an independent body reporting to the President’s Foreign Intelligence Advisory Board. See Exec.
Matters relating to FBI misconduct in counterintelligence activities are subject to investigation by the FBI’s Office of Professional Responsibility and by the Inspector General of the Justice Department. All FISA authorities and all national security letter authorities contain a congressional reporting requirement and fall within the oversight of the House and Senate intelligence committees. Despite common perceptions, therefore, FBI counterintelligence actually functions within a highly regulated environment, and the language of §215 explicitly invokes such oversight.

Another criticism concerns the lack in §215 of a requirement for notice to the individual whose records have been obtained. Without knowledge of the government’s actions, the individual cannot challenge the legality of those actions, nor can the individual resist the further use or dissemination of records obtained. Notice is not constitutionally required, however, where the government is obtaining information about a person from a third party outside the context of a criminal proceeding. There is also a broad policy reason for secrecy, and this is reflected in the integration of non-disclosure provisions into all counterintelligence legal authorities. Unlike criminal
investigations, where the existence of the investigation is often known publicly, or it is widely presumed since it follows a criminal act, counterintelligence operations typically cease to exist when they are revealed.\textsuperscript{191} The goal of counterintelligence is to detect and monitor the activities of the foreign power or its agent without the knowledge of the foreign power. If the counterintelligence operation is revealed, the government typically turns to overt tools like criminal investigations and prosecutions, immigration proceedings, administrative processes, or diplomatic activity to respond to a threat.

Secrecy has been recognized as essential since the very beginning of American intelligence operations.\textsuperscript{192} In many respects, the regulatory scheme governing counterintelligence, the higher legal standards for counterintelligence authorities, and even the “wall” separating intelligence and criminal law enforcement have all functioned to counter-balance and contain a tendency toward excessive secrecy in this area. The USA PATRIOT Act alters some of these constraints by lowering the legal standards for transactional information authorities and by largely dismantling the “wall.” It should certainly prompt a re-examination of some secrecy provisions. However, the operational and policy concerns that consistently tipped the balance in favor of secrecy, even during the counterintelligence reforms of the 1970s, are even more pressing in the post-9/11 environment.

My goal in Section II has not been to defend §215 against its critics, but rather to place those criticisms within the larger context of the counterintelligence legal authorities and the evolution of access to transactional information. The review of history in Section I and this contextualization in Section II are intended to better inform the revision of §215 proposed below.

**III. REVISIONING SECTION 215**

Within the next year, Congress will have to decide whether or not to retain §215 (along with other parts of the USA PATRIOT Act) in its present form. The sunset clause of the Act was intended to give Congress a chance to re-

---

\textsuperscript{191} In enacting the non-disclosure provisions for counterintelligence authorities, Congress appeared to accept this as axiomatic. \textit{See, e.g.,} H.R. REP. NO. 99-690(I), at 15 (“The FBI could not effectively monitor and counter the clandestine activities of hostile espionage agents and terrorists if they had to be notified that the FBI sought their financial records for a counterintelligence investigation.”).

\textsuperscript{192} In often-quoted directions to some of the first American intelligence operatives, George Washington wrote: “All that remains for me to add is, that you keep the whole matter as secret as possible. For upon secrecy, success depends in most Enterprises of the kind, and for want of it, they are generally defeated, however well planned and promising a favourable issue.” Letter to Elias Dayton, July 26, 1777, \textit{reprinted in} 8 \textsc{Writings of George Washington from the Original Manuscript Sources}, 1745-1799 (John C. Kirkpatrick ed., 1931-1944), \textit{available at} http://etext.virginia.edu/toc/modeng/public/WasFi08.html.
evaluate the necessity of these expanded authorities. In the case of §215, it appears that Congress will have very little operational data upon which to base its decision. The FBI and Justice Department will doubtless continue to insist that the capability provided by §215 is necessary, even if it is rarely employed. Critics of the Act will argue that the potential for abuse is so great that it should be eliminated or severely curtailed. Both sides begin from sound premises. The nature of the terrorist threat demands that our counterintelligence legal tools be effective, flexible, and readily available. However, these tools also represent compulsory, secret government access to personal information, and therefore they should be available only under conditions that minimize their potential for abuse.

I suggest that by drawing from the evolution of these tools and other counterintelligence authorities over time, §215 can be revised to accommodate the concerns of both sides. I make two assumptions in proposing these revisions. First, I assume that the FBI will continue to have an actual need for the general capability to compel production of transactional information, beyond that already provided for in national security letter and FISA pen register authorities. Some might argue that the USA PATRIOT Act’s near-complete demolition of the “wall” between counterintelligence and criminal investigations renders the “business records” authority entirely unnecessary. Now that sharing of grand jury information with the intelligence community is permitted, it could be said, counterintelligence agents who encounter the need for business records can simply use grand jury subpoenas to obtain them. I find that view unconvincing for several reasons. Although the USA PATRIOT Act permits the sharing of grand jury information under certain circumstances, it does not compel it. The availability of a grand jury also depends upon the existence of an open criminal investigation; counterintelligence operations address many situations in which there is not yet sufficient indication of criminal activity to open such an investigation. Finally, although the grand jury sharing provision in the USA PATRIOT Act

194. See supra note 6. Although it is possible that the FBI has used §215 since September 18, 2003, the fact that the FBI made no use of the authority in the two years immediately following the September 11 attacks (presumably a period of high investigative activity) is telling.
197. Section 218, which added the “significant purpose” language to FISA, is subject to the sunset provision. See Pub. L. No. 107-56, §§218, 224(a); supra note 24.

198. The FBI apparently has sought library records by voluntary production. See Letter from Assistant Attorney General Bryant to Senator Leahy, supra note 173, encl. at 2.
would accommodate other statutes controlling the privacy of particular types of information. Should Congress decide to protect library records specifically, or any body of transactional information, the business records authority could continue to function. Similarly, the language would not require alteration should the Supreme Court revisit Miller or otherwise modify the notion of transactional information. This new language would alleviate concerns over the scope of the authority and over the expansiveness of the “relevance” standard. The court would be in a position to detect and terminate unwarranted “fishing expeditions.” Decisions of the FISA judge on these applications would be subject to review by the Foreign Intelligence Surveillance Court of Review established in §103(b) of FISA, thus allowing further refinement of the legal standard.

My second revision would address the question of notice to the person to whom the information pertains. While the counterintelligence value of the authority would vanish if notice were commonly required, there is precedent for giving the affected person notice when the government uses the information for a purpose other than counterintelligence. The other three FISA-based counterintelligence authorities (electronic surveillance, physical search, and pen register/trap and trace) all contain provisions restricting the use and dissemination of information gained through the FISA authority, requiring notice to the person affected if the government intends to “enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States” information so obtained, and giving the aggrieved party a specific procedure through which to challenge the use of the information in a criminal proceeding. The text of these provisions could easily be inserted into the business records section, with the phrase “business records order” replacing the phrase “pen register or trap and trace device” throughout. This change would defuse some of the criticism over notice, and it would allow for the development of additional case law as application of the authority was examined in the criminal courts.

199. 50 U.S.C. §§1806 (electronic surveillance), 1825 (physical search), 1845 (pen register/trap and trace).
200. This language, found in the pen register section, 50 U.S.C. §1845(c), is typical.
201. The procedure is designed to afford the government an opportunity to protect sensitive national security information while allowing the defendant to challenge the legality of the particular application of the FISA authority. See, e.g., 50 U.S.C. §1845(e)-(h).
202. The notice and challenge provisions for FISA pen registers (50 U.S.C. §1845) have yet to be examined in the context of a criminal case, but the analogous provisions for FISA electronic surveillance (§1806) have been. See United States v. Isa, 923 F.2d 1300, 1305-1307 (8th Cir. 1991); United States v. Badia, 827 F.2d 1458, 1462-1464 (11th Cir. 1987); United States v. Ott, 827 F.2d 473, 475-477 (9th Cir. 1987); In re Kevork, 788 F.2d 566, 568-571 (9th Cir. 1986); United States v. Beltfield, 692 F.2d 141, 143-149 (D.C. Cir. 1982); United States v. Megahey, 553 F. Supp. 1180, 1193-1194, 1196-1197 (E.D.N.Y. 1982), aff'd sub nom. United States v. Duggan, 743 F.2d 59 (2nd Cir. 1984); United States v. Falvey, 540 F. Supp. 1306, 1315-1316 (E.D.N.Y. 1982).
These two revisions, if adopted, would place §215 more firmly in the tradition of carefully circumscribed counterintelligence authorities. Like national security letters and the FISA pen register authority, the scope of §215 authority would then be defined as limited to transactional materials. The definition, of course, would be dynamic, shaped by the action of the courts. The authority therefore could remain flexible, while concerns about its application to protected data would be removed. The revisions would also maintain the principle that the use of counterintelligence authorities calls for greater control than does application of analogous criminal investigatory approaches. The revised authority would function at roughly the legal standard of the grand jury subpoena, but with direct, rather than indirect, judicial oversight.

The changes proposed in this article, or something like them, are essential if Congress chooses to retain §215. The law as written simply does not inspire sufficient confidence to overcome the fear of abuse. During the congressional debates on the USA PATRIOT Act, there was extensive quotation of revered patriots, led by a warning attributed to Benjamin Franklin that “if we surrender our liberty in the name of security, we shall have neither.”

Franklin’s actual words are more nuanced and present a more direct challenge to §215 in its present form: “Those who would give up essential Liberty, to purchase a little temporary safety, deserve neither Liberty nor Safety.”

Careful attention to the actual history of counterintelligence authorities, arcane and inaccessible though it may be, will yield the raw materials needed to construct an effective, balanced authority to replace the current §215. An appropriate narrowing of the statute will both protect what is essential to our freedoms and enhance our long-term security.

