2005

Are There Any Checks And Balances On The Government’s Power To Check Our Balances? The Fate Of Financial Privacy In The War On Terrorism

Eric J. Gouvin

Western New England University School of Law, egouvin@law.wne.edu

Follow this and additional works at: http://digitalcommons.law.wne.edu/facschol

Part of the Banking and Finance Commons

Recommended Citation

ARE THERE ANY CHECKS AND BALANCES ON THE GOVERNMENT'S POWER TO CHECK OUR BALANCES? THE FATE OF FINANCIAL PRIVACY IN THE WAR ON TERRORISM

by ERIC J. GOUVIN*

In the three years since the terrorist attacks of September 11th, 2001, the laws affecting money laundering and financial privacy in the United States have been changed to give law enforcement agencies easier access to financial information. Although the changes to the law were passed with the claim that they were needed to intercept terrorist financing, the anti-money laundering provisions enacted by the USA PATRIOT Act are being used routinely against non-terrorist criminal suspects as part of regular law enforcement processes. Although the apprehension of ordinary criminals by any means available will sound perfectly acceptable to many, it is at odds with our traditional approach to financial privacy. This paper concludes that Congress ought to revisit the money laundering regime to make sure it strikes the appropriate balance between the legitimate desire for financial privacy and the legitimate need for law enforcement access to suspicious accounts. After review, lawmakers may find that procedural adjustments to provide protection from law enforcement abuse of the system are called for.

INTRODUCTION

"See, 9/11 changed everything."1

The events of September 11, 2001 brought about many changes in both domestic and foreign policy. Among other things; they changed the official American approach to anti-money laundering regulation. While historically our anti-money laundering laws had been geared primarily toward tracing the proceeds of crime, after September 11th, government officials began touting anti-money laundering rules as an effective technique for intercepting terrorist financing in order to prevent criminal acts from happening in the first place.

Using the war against terror as a justification, the changes in anti-money laundering law came in rapid succession in the fall of 2001.2 Within two weeks of

---

* Associate Dean of Academic Affairs and Professor of Law, Western New England College School of Law, Springfield, Massachusetts.


2. See Michael P. Malloy, Commentary, Panel One: Unfunding Terror—Perspectives on Unfunding Terror, 17 TRANSNAT’L L. 97 (2004) (summarizing the major changes implemented in the
the terrorist attacks, President Bush issued Executive Order 13224 freezing the assets of, and prohibiting transactions with, persons who commit, threaten to commit, or support terrorism.\(^3\) Two weeks later, the G-8 finance ministers agreed to pursue a comprehensive strategy to disrupt terrorist financing\(^4\) and by October 6, 2001, had implemented an action plan to do so.\(^5\) By the end of October, the Financial Action Task Force (FATF), an international intergovernmental anti-money laundering body, started developing guidance for financial institutions aimed at detecting the techniques and mechanisms of terrorist financing.\(^6\)

Stateside, on October 26, 2001, less than six weeks after the September 11th attacks, President Bush signed into law the USA PATRIOT Act\(^7\) (the "Patriot Act"), which included, within its 342 pages, Title III—the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001.\(^8\) At the time of the law's passage, legislators across the political spectrum, from Rep. Bob Barr on the right to Rep. Barney Frank on the left, warned of the Patriot Act's potential for loss of privacy.\(^9\) Nevertheless, in the heat of the moment, the massive bill was adopted with very little opposition.

With the perspective gained during the three years since its enactment, policy analysts now have the opportunity to examine the Patriot Act without the September 11th attacks as the immediate emotional backdrop. By any fair measure, the Patriot Act brought about dramatic changes in the law. Although

\(^3\) Exec. Order No. 13,224, 66 Fed. Reg. 49, 079 (Sept. 23, 2001) (hereinafter E.O. 13224). The order was extraordinary in its scope in a couple of ways. It froze assets and prohibited transactions with a poorly defined group of persons who are "otherwise associated" with any designated terrorist. Id. at Sec. 1(d)(iii). In addition, the White House maintained that the order gave the Treasury Department the power to "block the U.S. assets of, and deny access to U.S. markets to, foreign banks who refuse to freeze terrorist assets." The White House Office of the Press Secretary, Fact Sheet: Executive Order on Terrorist Financing, Sept. 24, 2001, available at http://www.whitehouse.gov/news/releases/2001/09/20010924-2.html.


many commentators have concluded that the Patriot Act goes too far, during the 2004 presidential campaign pointing out problems with the law during the 2004 presidential campaign seemed to be considered by some an act akin to treason.\textsuperscript{10} Now that the election is behind us, the time may be at hand to re-evaluate this hastily-enacted legislation in light of our traditional values of financial privacy and limited government intrusion into personal business.\textsuperscript{11} After a full public discussion, we may decide that the Patriot Act tipped the balance in favor of law enforcement agencies in a way that we have not considered prudent in the past.

The first part of this article sketches out the tension between financial privacy and the need for law enforcement access to private financial information that existed prior to the passage of the Patriot Act. The second part describes how the Patriot Act changed the law of financial privacy. The third part discusses how the expanded law has actually been used by law enforcement officials. The fourth part discusses various options for dealing with the Patriot Act's changes to financial privacy in order to bring the law more into line with traditional values in this area.

I. FINANCIAL PRIVACY LAW PRIOR TO THE PATRIOT ACT

Over the past thirty years or so our policy makers have been trying to find the right balance between a financial institution customer's legitimate desire for financial privacy and law enforcement agencies' legitimate need for access to financial records.\textsuperscript{12} In general, although there is no federally recognized "expectation of privacy" in bank records for the purposes of the Fourth Amendment,\textsuperscript{13} bank customers do in fact have a common law right to financial privacy implicit in the contract between the bank and its customer.\textsuperscript{14} Historically,
bank customers have expected their bank records to be held in confidence. In 1970, against this backdrop of the common law of financial privacy, Congress passed the law which became the cornerstone of our anti-money laundering policy, the "Bank Secrecy Act" ("BSA").

The BSA requires banks and other "financial institutions" to keep certain records and authorizes the Secretary of the Treasury to require those institutions to report certain financial transactions. The stated policy reason for the Bank Secrecy Act is: "Such records and reports are of a high degree of usefulness in criminal, tax, and other regulatory investigations." The regulations implementing the BSA originally required covered financial institutions to report each deposit, withdrawal, exchange of currency, or other payment or transfer which involved a transaction in currency of more that $10,000.

Shortly after its enactment, skeptics of the BSA's approach to anti-money laundering pointed out that it was relatively easy to evade the law since it only applied to transactions of $10,000 or more and did not cover all types of financial intermediaries. Indeed, in the thirty plus years since its implementation, policy makers have continually tinkered with the rules to try to address those shortcomings. At the time of its enactment, however, the most important objection to the BSA was that the law was inconsistent with bank customers' condition without consent had a claim based on breach of an implied contract that bank would not disclose information concerning depositor's account to third parties unless authorized by law or depositor.

15. In four special circumstances, however, the implied contract right of privacy is limited: (1) disclosure under compulsion of law; (2) disclosure pursuant to the public interest; (3) disclosure pursuant to the bank's interest; and (4) disclosure pursuant to the customer's express or implied consent. Milohnich, 224 So. 2d at 761. The common law of financial privacy does not apply to checks, since they are given to strangers and generally circulated, nor to bank records made by the bank for its own purposes. ALFRED M. POLLARD, BANKING LAW IN THE UNITED STATES §5.2 (1992). In addition, there is authority for the proposition that a bank may have a duty to disclose otherwise confidential information to a customer with which it has a fiduciary relationship. See Barnett Bank of W. Fla. v. Hooper, 498 So. 2d 923, 925 (Fla. 1986) (holding that a bank which enters into a transaction with "a customer with whom it has established a relationship of trust and confidence, and it is a transaction from which the bank is likely to benefit at the customer's expense" the bank could have assumed "a duty to disclose facts material to the transaction" that are not available to the customer); Catalina Yachts v. Old Colony Bank & Trust, 497 F. Supp. 1227, 1236 (D. Mass. 1980) (holding that a bank cannot practice selective disclosure which is "designed to misrepresent the financial status of its customer").


20. The regulations promulgated by the Department of Treasury under the Bank Secrecy Act are found at 31 CFR §103.11 (2004). Over the years they have been expanded to cover related transactions which in the aggregate exceed $10,000 and other situations to reduce the chance for evasion.


22. For example, banks are now required to institute compliance procedures to aggregate transactions under $10,000 in order to detect and prevent evasion of the BSA rules. 31 U.S.C.A. § 5324 (West 2003).
expectations of privacy. Ultimately, the United States Supreme Court, in a majority opinion written by Justice Rehnquist, declared that the BSA was constitutional because there was no reasonable expectation of privacy in the bank/customer relationship with regard to information required by the government.\textsuperscript{23} In the delicate balance between financial privacy and the need for law enforcement agencies to obtain information, the Court tipped the scales in favor of law enforcement.

As if to demonstrate that the American approach to financial privacy was a true balancing act, 1970 saw the passage of the Fair Credit Reporting Act (FCRA),\textsuperscript{24} which sought to safeguard consumer financial information. Congress’ enactment of the FCRA was a response to the perception that some credit bureaus engaged in unfair practices in the collection and reporting of personal credit data and other information.\textsuperscript{25} The FCRA required credit bureaus to respond to consumer complaints and limited the availability of consumer credit reports only to specific “permissible purposes.”\textsuperscript{26} So, while the BSA whittled away at personal financial privacy, the FCRA sought to protect it. This pattern of give-and-take in the area of financial privacy has played out ever since those important Acts were made law.

The next important statute affecting financial privacy was the Right to Financial Privacy Act (the “Privacy Act”),\textsuperscript{27} passed in 1978. The Privacy Act was designed to counteract some of the invasive aspects of the BSA. Generally, the Privacy Act prohibits disclosure of a customer’s individual\textsuperscript{28} financial records to a government authority without the customer’s consent.\textsuperscript{29} The Privacy Act provides broad coverage for financial privacy subject to many exceptions. While the

\textsuperscript{23} California Bankers Association v. Schultz, 416 U.S. 21, 52-54 (1974) (holding that the Bank Secrecy Act’s recordkeeping and reporting requirements do not deprive financial institutions of due process, nor does the implementation of the BSA constitute an illegal search and seizure in violation of the Fourth Amendment); Miller, 425 U.S. at 441-443 (1976) (holding that there is no Fourth Amendment expectation of privacy in a person’s bank records when a government agency has an interest in examining those records).


\textsuperscript{25} Congress was aware of the impact of Miller and the Right to Financial Privacy Act was in part a response to that decision. H.R. REP. NO. 95-1383, at 34 (1978), reprinted in 1978 U.S.C.C.A.N. 9273, 9306. “In the celebrated Miller case, the Supreme Court held that the fourth amendment prohibitions against search and seizure did not protect bank records . . . . The Court did not however, rule out a legislative remedy to this very large hole in the constitutional privacy protections of individuals.” 124 CONG. REC. S37,570 (daily ed. Oct. 14, 1978) (statement of M. Abourezk) (emphasis added).

\textsuperscript{26} 15 U.S.C. § 1681b (defining the purpose of the subchapter as requiring consumer reporting agencies to “adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of this subchapter”).


\textsuperscript{28} The law protects individuals and partnerships consisting of five or fewer individuals, but does not extend to corporations. 12 U.S.C.A. § 3401(4) (West 2001 & Supp. 2002).

\textsuperscript{29} 12 U.S.C.A. § 3402(1) (West 2001 & Supp. 2002). Among other exemptions found in section 3413, the Act does not prohibit disclosure in the following situations: (1) where the financial information is not individually identifiable, § 3413(a); (2) where the financial institution itself is being investigated, § 3413(b); and (3) where the disclosure is in accordance with Internal Revenue Code provisions or other federal statutes or rules. §3413(c).
Privacy Act establishes that the government does not have unfettered access to customer bank accounts, it also provides that a customer may authorize disclosure to a government authority, subject to revocation.\(^\text{30}\)

Even with the protections contained in the Privacy Act, however, the government could obtain access to financial records without the customer's consent pursuant to an administrative subpoena, a judicial subpoena, a search warrant, and, in certain circumstances, a formal written request.\(^\text{31}\) Under the Privacy Act a customer is ordinarily entitled to notice before disclosure to a government authority,\(^\text{32}\) and has the right to challenge the disclosure.\(^\text{33}\) Although critics of the Patriot Act have complained about delayed notification of government action, it is worth noting that the Privacy Act provided for delayed notice to the customer pursuant to court order if giving notice would have resulted in the flight of the customer from prosecution, destruction of evidence, intimidation of potential witnesses, or the serious compromising of an investigation or proceeding.\(^\text{34}\) Even before the attacks of September 11th, special procedures under the Privacy Act governed access to financial records in connection with certain intelligence activities.\(^\text{35}\)

Throughout the 1980s\(^\text{36}\) and 1990s,\(^\text{37}\) Congress made adjustments to the basic schemes of financial privacy and financial reporting, but the fundamental tension between the two regulatory schemes remained—some provisions pushed for greater privacy while others pushed for greater access by law enforcement officials. In 1998, however, it seemed that the delicate balance between the two competing policies was in danger of being lost. Banking regulators attempted to push the balance in favor of government access to private financial information, with the so-called "Know Your Customer" ("KYC") proposal, which would have required banks to closely monitor customer activity.\(^\text{38}\) Among other things, the 1998 KYC

31. § 3402(2)-(5).
32. § 3408(4).
33. § 3410(e).
34. §§ 3409(a)(3)-(b)(3).
35. § 3414.
37. In 1992, for instance, Congress passed the Annunzio-Wylie Anti-Money Laundering Act. 102 Pub. L. No. 550, 106 Stat. 3672 (codified as amended in scattered sections of 12, 18, 31 and 42 U.S.C.A.). This Act further bolstered the requirements of the BSA by requiring the filing of "Suspicious Activity Reports" (known in the industry as SARs) that were "relevant to a possible violation of law or regulation." 31 U.S.C.A. § 5318(g)(1) (West 2003). SARs were an attempt to fine tune the money laundering reporting system in light of the fact that a bright line dollar amount rule sometimes left suspicious transactions unreported. If a transaction is "suspicious" it must be reported. A transaction is considered suspicious if it involves an aggregate amount of $5000 or more. 31 C.F.R. § 103.18(a)(2) (2004).
In response to the proposed rules, the federal banking regulators received a flood of comment letters, the overwhelming majority of which opposed the rules. The proposed rules were withdrawn in March of 1999.

The political fallout from the over-reaching KYC proposal was quite significant. After the KYC debacle, Congress spent a great deal of time and effort bolstering the right of financial privacy. Title V of the Gramm-Leach-Bliley Act of 1999 ("GLB Act") addressed several matters relating to the protection of nonpublic personal information of customers of financial service providers. The GLB Act mandated the issuance of comprehensive regulations to be promulgated by the federal banking regulators, the FTC and the SEC, in consultation with state insurance regulators, to protect the confidentiality and safeguard the security of the personal consumer information maintained by financial institutions.

The GLB Act specifically permits customers of financial institutions to opt out of having their information shared with any unaffiliated third party. In addition, financial institutions are prohibited from disclosing certain types of information, such as account numbers and access codes, to unaffiliated parties in any event. As required by the law, the Office of the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision jointly published final regulations to implement the privacy provisions contained in the GLB Act.


GLB Act § 504. It is important to note that the GLB-mandated privacy provisions do not entirely preempt state privacy laws. Andrea Lee Negroni & John P. Kromer, Gramm-Leach-Bliley: Tip of the Privacy Iceberg, 118 BANKING L.J. 958, 959 (Nov. 2001). In many cases existing state privacy laws affecting financial institutions are more restrictive than the GLB provisions and may not be completely preempted by the GLB Act. Id.

GLB Act § 502(a), (b).

§ 502(a), (b).

Privacy of Consumer Financial Information, 65 Fed. Reg. 35,162 (June 1, 2000) (codified at 12 C.F.R. pts. 40, 216, 332, 573). Among other things, the final regulations require financial institutions to: (1) provide customers with a notice of the institution's privacy policies and practices, with the initial disclosure for new customers being provided no later than when the customer relationship is established; (2) provide customers with the opportunity to opt out or bar the institution from sharing customer information with unaffiliated third parties unless the institution has a reasonable basis to believe that the information is lawfully publicly available from certain public sources; (3) refuse to disclose account information to third-party marketers unless it is an account to which no charge can be posted or the
The GLB Act’s enhanced privacy provisions were the last installment in the back and forth struggle between privacy advocates and law enforcement advocates before the attacks of September 11th precipitated the passage of the Patriot Act, with its major changes to U.S. money laundering law. That last installment clearly showed that financial privacy was the stronger value in the late 1990s and that politically it was an important issue.

Then came September 11th, and everything changed. Law enforcement officials seized on anti-money laundering rules as valuable tools in terrorist investigations and sought to liberalize law enforcement access to financial records.\(^{48}\) It should be noted that although the anti-money laundering provisions of the Patriot Act appeared to be a response to the terrorist attacks, those provisions were not in fact new. The money laundering provisions that became Title III of the Patriot Act had been floating around Congress for several years prior to September 11th. Congress had even held hearings on various proposals to enhance money laundering rules, but, largely due to civil liberties concerns, it did not pass any new anti-money laundering legislation in the years immediately preceding the passage of the Patriot Act in 2001.\(^{49}\) It was not, however, for lack of trying.

In the period 1998-2001 many proposals for enhanced money laundering efforts were made, but prior to September 11th, proponents of tougher anti-money laundering legislation could not make the case for passage of those bills. A review of the Thomas website at the Library of Congress reveals that in the 105\(^{th}\) Congress (1997-1998), the following bills were considered, although none of them were enacted into law: The Money Laundering Act of 1998,\(^{50}\) The Money Laundering Deterrence Act of 1998,\(^{51}\) and the Money Laundering Enforcement and Combating Drugs in Prisons Act of 1998.\(^{52}\) The 106\(^{th}\) Congress (1999-2000) also saw a flurry of proposals for enhanced money-laundering rules, none of which were enacted into law. These included the Money Laundering Prevention Act of 1999,\(^{53}\) the

---

50. Money Laundering Act of 1998, H.R. 3745, 105th Cong. (1998). This bill died in committee. Bill Summary available at http://thomas.loc.gov (follow “Bill, Resolutions” hyperlink on the left, then follow “Search Bill Summary & Status” hyperlink in the middle of the page, then follow “Search Multiple Congresses” hyperlink on the upper right, then select box for “105th Congress” and enter the title of the bill into the search box).
Foreign Money Laundering Deterrence and Anticorruption Act,\textsuperscript{54} the Money Laundering Abatement Act of 1999,\textsuperscript{55} the Integrity in Banking and Money Laundering Prevention Act of 1999,\textsuperscript{56} the Money Laundering Act of 2000,\textsuperscript{57} the International Counter-Money Laundering Act of 2000,\textsuperscript{58} and the International Counter-Money Laundering and Foreign Anticorruption Act of 2000.\textsuperscript{59} It is clear that in the years leading up to the September 11th attacks, Congress was entertaining the idea of increased anti-money laundering rules, but did not yet have the political critical mass to pass an acceptable bill.

In summary, prior to the passage of the Patriot Act, the U.S. anti-money laundering system worked on the assumption that the typical money laundering problem arose along the lines of the following scenario: a criminal either committed a crime and got a lot of money or dealt with other criminals and got a lot of money. The criminal then took that tainted money to a financial institution. The financial institution might consider the transaction with the customer noteworthy either because: (1) it exceeded the $10,000 transaction limit under the BSA; (2) it was part of a series of transactions structured in such a way as to avoid the $10,000 BSA limit; or (3) it was over $5,000 and was “suspicious.” If the transaction raised a red flag, the financial institution filed either a “currency transaction report” (“CTR”) or a “suspicious activity report” (“SAR”) with the Financial Crimes Enforcement Network (“FinCEN”), putting the law enforcement community on notice of a potentially noteworthy transaction that might deserve closer attention. Using data management techniques, FinCEN could then process this data to find patterns that would lead the law enforcement agencies to bring the criminals to justice and prevent them from committing any more crimes.

In theory, the scheme described above makes sense and presents a coherent vision of how a sacrifice in financial privacy can result in a balancing benefit in more effective law enforcement. In practice, however, this one-way reporting system has not worked very well. Built-in incentives for financial institutions to

\textsuperscript{54} Foreign Money Laundering Deterrence and Anticorruption Act, H.R. 2896/S. 1663, 106th Cong. (1999). These bills died in committee. See bill summaries, available at http://thomas.loc.gov. However, many of the provisions of the bill ultimately ended up in Title III of the Patriot Act; see 147 CONG. REC. H7201 (daily ed. Oct. 23, 2001) (statement of Rep. LaFalce) (describing his prior legislation as giving the Secretary of the Treasury the power to “block transfers of funds into the United States financial system from foreign banking systems that are easily exploited by terrorists and criminal organizations because those foreign jurisdictions have weak or nonexistent anti-money laundering regimes”).


\textsuperscript{58} International Counter-Money Laundering Act of 2000, H.R. 3886, 106th Cong. (2000). This bill was reported out of committee but no floor action was taken. See Bill Summary, available at http://thomas.loc.gov.

over-report transactions\textsuperscript{60} result in an incredible amount of information overload on the anti-money laundering system.\textsuperscript{61} Sifting through and making sense of all the financial data that comes to FinCEN is a Herculean task, and one which has not been successfully executed in the past. While it may be possible for FinCEN to rise to the challenge by employing state-of-the-art data mining techniques and predictive technology like that currently used in the private sector,\textsuperscript{62} much depends on whether FinCEN will have the personnel and resources to implement such a sophisticated arrangement.\textsuperscript{63} But all of that was before the Patriot Act changed the fundamental dynamic of the anti-money-laundering scheme.

II. HOW THE PATRIOT ACT CHANGED THE LAW

The money laundering provisions found in Title III of the Patriot Act changed our system of money laundering in a fundamental way.\textsuperscript{64} Prior to the passage of

\begin{itemize}
  \item 60. The BSA imposes strict liability for failure to file appropriate reports. 31 U.S.C.A. § 5321(a)(3)(2002). See U.S. v. Bank of New England, 821 F.2d 844, 855-57 (1st Cir. 1987) (ruling that the bank had the requisite mental state if it deliberately avoided learning CTR requirements). On the other hand, there is no liability attached to filing extraneous reports in good faith. See Lopez v. First Union Nat'l Bank of Fla., 129 F.3d 1186, 1192-93 (11th Cir. 1997) (explaining that the good faith exception encourages financial institutions to play a role in combating money laundering); Brown v. Nationsbank Corp., 188 F. 3d 579, 589 (5th Cir. 1999) (stating that "[i]f private businesses were not eligible for immunity from state law claims arising from assisting undercover federal operations, this would provide a major disincentive to assisting law enforcement and would undermine the needs and interests of the federal government"). Indeed, our money laundering law contains a provision holding reporting entities free from liability in connection with the filing of suspicious activity reports. 31 U.S.C. §§ 5318(g)(3)(A) (2002) (Persons reporting suspicious activity "shall not be liable to any person under any law or regulation of the United States . . . or of any State . . . for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure"); see Palmer Paxton Stoutt v. Banco Popular de Puerto Rico, 320 F.3d 26, 33 (1st Cir. 2003) (upholding summary judgment in favor of bank that filed SAR in connection with a customer who allegedly obtained funds under fraudulent pretenses on the grounds that the safe harbor of 31 U.S.C. § 5318(g)(3) protects the bank). The Patriot Act also gives reporting institutions the same protection. Patriot Act § 351, 31 U.S.C.A. § 5318(g)(3) (2002).
  \item 61. FinCEN estimates that thirty-percent of the twelve million currency transaction reports it received in 2001 were filed unnecessarily. Rob Garver & Michele Heller, In Brief: FinCEN Seeks Streamlined Filing Process, AM. BANKER, Sept. 5, 2002, at 3. According to a FinCEN press release: "These millions of excess forms have little value for law enforcement purposes and, we believe, impose substantial compliance costs upon financial institutions. . . . Also, excess filings burden our intelligence analysis and impede timely targeting of money laundering, terrorist financing, and other vulnerable transactions." Id.
  \item 62. See Mike France, et al., Privacy in An Age of Terror, BUS. WK., Nov. 5, 2001, at 83, 84 (outlining the technology available to help combat terrorist threats and the effect of those technologies on privacy).
  \item 63. Industry observers are certainly skeptical that FinCEN will be able to process the data in real time to actually intercept terrorist acts, especially where on-line transactions are involved. See Steve Zelinger, Commentary, Panel One: Unfunding Terror—Perspectives on Unfunding Terror, 17 TRANSNAT'L LAW 119, 123 (2003) (former Senior Counsel to Visa International expressing doubt that companies or the government have the technical capability to process the amount of data called for under the money laundering rules).
  \item 64. For a tidy summary of the changes brought about by Title III of the Patriot Act, see Malloy, supra note 2, at 101-9.
\end{itemize}
the Patriot Act, the money laundering laws focused primarily on tracing the proceeds of crime as criminals sought to make those ill-gotten gains look legitimate.65 After the Patriot Act the ostensible goal of the anti-money laundering statutes is to intercept the financing of criminal acts before they ever take place.66 Post September 11th, our elaborate system of anti-money laundering provisions proceeds on the assumption that it is possible to prevent terrorist activities by “connecting the dots” in the financial transactions reported under our laws.67

The biggest challenge confronting law enforcement officials as they try to connect the dots is knowing which dots are important enough to be connected. Under the pre-Patriot Act anti-money laundering rules, the law enforcement community had a flood of data and was trying to separate the important transactions from the noise. Prior experience with this approach showed that it did not always work well. When law enforcement officials try to find patterns in the flood of data that flows to FinCEN, they often end up with false positives. In two of the most notorious examples, radio personality Rush Limbaugh was investigated for money laundering in connection with his oxycontin addiction,68 while former Senator Bob Dole raised money laundering concerns in light of his personal predilection for carrying around large wads of cash.69

Of course, it would be much easier for law enforcement officials to intercept crime if, instead of having to identify possible criminal suspects based on patterns in their financial dealings as reported under the BSA, they could turn the process around and start with a suspect and use the anti-money laundering system to see if the suspect has done anything wrong. This is what the Patriot Act allows law enforcement agencies to do. The Patriot Act permits the development of that strategy by virtue of three major changes in the regulatory scheme: (1) a dramatic expansion in the definition of “financial institution” under the BSA; (2) new “Know Your Customer” rules; and (3) the implementation of provisions requiring information sharing with law enforcement agencies and permitting information sharing among financial institutions.

A. The Definition of “Financial Institution”

The Patriot Act contains extensive provisions designed to improve the government’s anti-money laundering efforts. One of the common criticisms of the Bank Secrecy Act was that it was relatively easy to evade because it did not apply to all financial intermediaries, or applied in different ways to different

65. Id.
66. Id.
67. See Jimmy Gurulé, Commentary, Panel One: Unfunding Terror—Perspectives on Unfunding Terror, 17 TRANSNAT’L LAW. 113, 114 (2003) (former Undersecretary for Enforcement, U.S. Department of Treasury, stating that “with respect to the goal and purpose of the government’s terrorist financial strategy, it is preventative in nature”).
68. Mr. Limbaugh apparently was suspected of trying to avoid the BSA by structuring the withdrawals from his bank accounts to total less than $10,000 per transaction. CNN.com, Source: Limbaugh Investigated for Money Laundering, available at http://www.cnn.com/2003/SHOWBIZ/11/19/limbaugh.painkillers.ap/(last visited Dec. 15, 2005).
intermediaries. 70 So, for example, because banks were subject to relatively strong reporting requirements, many suspicious transactions migrated to less regulated channels. Cash transfer services like MoneyGram and Western Union became a favorite tool of criminals. 71 These networks could move cash very quickly and informally, with no need to set up an account and with minimal documentation requirements. 72 The Patriot Act corrected this problem by extending the reach of the BSA to a wide array of financial intermediaries, including, among others, licensed senders of money. 73 The Act's expansion of the financial institution

70. See Gouvin, supra note 21, at 964 (stating that not all financial intermediaries were subject to the BSA and that not all financial intermediaries were subject to the same requirements).

71. See Heather Timmons, Terrorist Money by Wire, BUS. Wk., Nov. 5, 2001, at 94 (discussing the appeal of money transfer services to criminals due to the looser regulatory requirements for providers).

72. See Heather Timmons, Western Union: Where the Money is—in Small Bills, BUS. Wk., Nov. 26, 2001, at 40-41 (discussing the speed and anonymity with which criminals are able to utilize money transfer services).

73. USAPA § 321 (amending the existing definition of “financial institution”), 31 U.S.C.A. § 5312(a)(2) (2002). Section 5312(a)(2) states:

(2) “financial institution” means—
(A) an insured bank (as defined in section 3(h) of the Federal Deposit Insurance Act (12 U.S.C. 1813(h)));
(B) a commercial bank or trust company;
(C) a private banker;
(D) an agency or branch of a foreign bank in the United States;
(E) any credit union;
(F) a thrift institution;
(G) a broker or dealer registered with the Securities and Exchange Commission under the Securities Exchange Act of 1934 (15 U.S.C. 78a et seq.);
(H) a broker or dealer in securities or commodities;
(I) an investment banker or investment company;
(J) a currency exchange;
(K) an issuer, redeemer, or cashier of travelers’ checks, checks, money orders, or similar instruments;
(L) an operator of a credit card system;
(M) an insurance company;
(N) a dealer in precious metals, stones, or jewels;
(O) a pawnbroker;
(P) a loan or finance company;
(Q) a travel agency;
(R) a licensed sender of money or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system;
(S) a telegraph company;
(T) a business engaged in vehicle sales, including automobile, airplane, and boat sales;
(U) persons involved in real estate closings and settlements;
(V) the United States Postal Service;
(W) an agency of the United States Government or of a State or local government carrying out a duty or power of a business described in this paragraph;
(X) a casino, gambling casino, or gaming establishment with an annual gaming revenue of more than $1,000,000 which—
(i) is licensed as a casino, gambling casino, or gaming establishment under the laws of any State or any political subdivision of any State; or
definition is an important innovation in anti-money laundering regulation. No longer can criminals get around the rules by using non-traditional channels. At the same time, law enforcement officials can gather a great deal of information on people through the wide range of enterprises which are now considered "financial institutions." The net is so broad, in fact, that law enforcement officials might easily put together quite a detailed profile of suspects based on information gathered through the various financial institutions that are now covered by the BSA. Combined with the two other provisions discussed below, this will prove to be part of an awesome investigatory power.

B. New "Know Your Customer" Rules

Another criticism of the pre-Patriot Act anti-money laundering regime was that the mechanical application of the statutory reporting rules resulted in many extraneous reports of very little value to the law enforcement community. Observers noted that the reporting system would produce more useful reports if the institutions generating the reports knew something about their customers' ordinary transactions in order to assess at the time of a reportable transaction whether the transaction was truly noteworthy or suspicious.74 This was the impetus behind the "Know Your Customer" proposal of 1998—essentially it was a bid to enlist financial intermediaries as spies for the government. The Patriot Act revisits the "Know Your Customer" idea, albeit in a somewhat watered-down form.

The Patriot Act directs the Secretary of Treasury to promulgate regulations establishing standards for financial institutions regarding the identity of customers opening accounts.75 The regulations implementing the Patriot Act require, among other things, that financial institutions implement reasonable procedures for: (1) verifying the identity of any person seeking to open an account, to the extent reasonable and practicable; (2) maintaining records of the information used to verify the person's identity, including name, address, and other identifying information; and (3) determining whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to the financial institution.

(ii) is an Indian gaming operation conducted under or pursuant to the Indian Gaming Regulatory Act other than an operation which is limited to class I gaming (as defined in section 4(6) of such Act);
(Y) any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any business described in this paragraph is authorized to engage; or
(Z) any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters.


74. See Gouvin, supra note 21, at 963-64 (describing "smurfing," an activity where large sums of money are deposited in smaller increments, which "led to a change in money laundering regulation designed to make bankers detect "suspicious" activities").

This represents a significant departure from previous law. Prior to the Patriot Act, banks were required to know their customer in only three specific situations: (1) to "verify and record the name and address of the individual presenting a transaction" when a CTR filing was required; (2) when customers purchased certain monetary instruments, such as cashier's checks and money orders; and (3) in certain wire transfers. Now presumably every customer is subject to the rules.

The expansion of the definition of "financial institution" together with the new Know Your Customer rules have tightened up the existing anti-money laundering scheme in ways that critics had been calling for for years. Those two changes make the system more difficult to evade and put financial institutions in a better position to assess when activity is "suspicious" enough to warrant a Suspicious Activity Report. These two changes would have gone a long way toward improving the anti-money laundering regime to make it more inclusive and to provide more useful information for law enforcement agencies without changing the underlying dynamic of the information flow. The third major change discussed below, together with the two already discussed, however, has the potential to change the entire dynamic of the anti-money laundering scheme.

C. Information Sharing Provisions

From the standpoint of financial privacy, the most powerful innovations in the Patriot Act are those provisions designed to encourage, or in some cases compel, the sharing of information among financial institutions, regulators and law enforcement authorities. Section 314(a) of the Patriot Act allows law enforcement agencies, acting through FinCEN, to gather information about the various financial arrangements of a person being investigated. Under the regulations implementing section 314, a federal law enforcement agency investigating either terrorist activity or money laundering may request that FinCEN provide certain financial information from a financial institution or group of financial institutions. FinCEN, in turn, can require financial institutions to search their records to ascertain whether they maintain or have maintained accounts for, or conducted transactions with, the individual or entity specified. The records requested might not have been problematic under existing anti-money laundering

76. 31 U.S.C.A. § 5318(t).
77. 31 C.F.R. § 103.28 (2001).
80. USAPA § 356(b); 31 C.F.R. §§ 103.90-110 (2004).
81. 31 C.F.R. § 103.100(b) (2004).
82. 31 C.F.R. § 103.100(b)(2004). While section 314 of the Patriot Act did not define "financial institution," the implementing regulations define "financial institution" for purposes of section 314 as any financial institution described in 31 U.S.C. 5312(a)(2) that is required under 31 CFR part 103 to establish and maintain an anti-money laundering program. 31 C.F.R. § 103.110(a)(2).
83. According to FinCEN, the section 314 request process allows law enforcement agencies to "reach out to 33,884 points of contact at more than 25,000 financial institutions to locate accounts and transactions..." Financial Crimes Enforcement Network, FinCEN's 314(a) Fact Sheet, Dec. 21, 2004, available at http://www.fincen.gov/314afactsheet122104.pdf.
rules—they could just be garden variety accounts.

The procedural safeguards for these inquiries are very modest. There is no requirement that the requesting agency have a search warrant, or a grand jury subpoena, or even an administrative subpoena. In short, there is no meaningful checking mechanism to prevent the abuse of the 314(a) power. All that the agency requesting the information needs to supply is identification information for the customer being searched, and a certification that the subject of the request is “engaged in, or is reasonably suspected based on credible evidence of engaging in, terrorist or money laundering” activity.84 While this sounds fine in the abstract, the concern comes in the execution.85

The section 314(a) mechanism works in the following way. Once it receives a request from FinCEN, a financial institution must “expeditiously” search its records for information relating to every individual, entity, or organization named in the request.86 If a financial institution does have a record of dealing with the subject of the inquiry, it must report back to FinCEN the following information: the name or account number of each individual or entity for which a match is found and a social security number and date of birth, or other similar identifying information that was provided by the subject of the information when the account was opened or the

84. 31 C.F.R. §103.100(b) (2004).
85. How the law enforcement community defines “credible evidence” is entirely within their discretion. A brief excerpt from the popular radio program A Prairie Home Companion illustrates the problem of over-zealous law enforcement agents seeing terrorists under every rock. In the skit, Detective Guy Noir (indicated in the script by the initials GK) is being interrogated by Harriet Hammer, an agent of the Homeland Security Department (indicated in the script by the initials SS). Agent Hammer is describing to Mr. Noir an important indicator of terrorist propensities:

SS: We have a program called Eccentric Lawn Care Advisory, or ELCA. We keep track of people who aren’t raking their leaves or cleaning their gutters or covering their flowers. Those things fit a terrorist profile.

GK: Terrorists?

SS: If they’re not doing their yardwork, then what are they doing? They could be online, conspiring with other members of their sleeper cell, planning a shoe attack.

GK: What’s that?

SS: Shoe bombs. Exploding sneakers. We’ve got an orange alert right now on older women with binoculars who are wearing oxfords.

GK: Those are birdwatchers.

SS: Could be, or they could be planning something involving the use of chickadees with explosives strapped to them. Anyway, poor lawn care is an important indicator. Anytime we find people with Scandinavian last names who aren’t blowing the leaves off their driveways, we put them under surveillance.

GK: That’s ethnic profiling.

SS: All I know is that when we see a lawn that’s full of leaves and the last name ends in -son or -sen or -quist or -rud or -strom, we have reason to believe they are sowing the seeds of hatred and trying to destroy democratic institutions.

GK: And?

SS: We pick em up. We bring em in.

86. 31 C.F.R. § 103.100 (b)(2)(i) (2004).
Financial institutions of which FinCEN makes information requests may not disclose the fact that FinCEN has requested or obtained information under section 314(a) to anyone, other than to FinCEN or the requesting agency, except when such disclosure is necessary to comply with the request. The Treasury Department takes the position that the information received from a financial institution under section 314(a) is information required to be reported in accordance with a federal statute or rule, and therefore is not barred under section 3413(d) of the RFPA or section 502(e)(8) of the GLB Act.

While the actual data provided under section 314 can be quite mundane and unexciting, the section 314 request mechanism that allows law enforcement agencies to narrow the field of potential financial institutions is quite dramatic. Instead of relying on reported transactions to raise suspicions about the activities of specific people, the regulations implementing section 314 allow FinCEN to request transaction information about an individual it considers suspicious regardless of any activities that person may have engaged in. Under the new approach, it is unlikely that transactions reported under the BSA will make the law enforcement agencies suspicious, but rather, it is suspicion that will lead law enforcement to want to examine the bank records. This turns our traditional system on its head.

The money laundering information flow has now become a two-way street. Unlike the pre-Patriot Act days where the information flowed in only one direction—from financial institutions to FinCEN—now the information can flow from FinCEN to the financial institutions as well. Prior to the development of section 314, law enforcement could look at the bank records of suspicious individuals only after establishing some plausible reason to suspect that individual was involved in criminal activity. Having identified the individual, the law enforcement authorities could then proceed to subpoena the individual’s financial institutions—if it could figure out which institutions were worth subpoenaing. Now, however, life is much simpler for the law enforcement side, as they can query all financial institutions through section 314.

The changes wrought by the Patriot Act have fundamentally altered the balance between privacy interests and law enforcement interests. In the words of Assistant Attorney General Michael Chertoff in testimony before the Senate Banking Committee: “the principal provisions of the Right to Financial Privacy Act no longer apply to letter requests by a government authority authorized to conduct investigations or intelligence analysis for purposes related to international terrorism.”91 As Mr. Chertoff understands the Patriot Act, law-enforcement officials investigating terrorist activities no longer even have to file a subpoena when requesting bank records.92

92. Id.
In addition to the "two way street" aspect of section 314(a), section 314(b) provides a safe harbor from liability for violation of financial privacy protections in order to permit information sharing among financial institutions. In order to take advantage of the safe harbor provisions, institutions must give an annual notice to FinCEN prior to sharing.93 The safe harbor protection provided by section 314(b) applies only to the sharing of information related to terrorist or money laundering activity.94 Sharing information regarding overdrafts, failure to pay child support, unemployment, bankruptcy, etc., is not covered by section 314(b) and should not be shared by financial institutions. Nevertheless, observers worry that increased exchanges among institutions along with the use of sophisticated profiling programs will further erode financial privacy.95

Some banking observers suggest that bankers will feel pressure to voluntarily obtain certification and share customer information in order to show that the institution is a "good citizen."96 That good citizen status could come in handy if the institution runs afoul of the arcane rules of money laundering and is faced with an enforcement action.97 Good citizen status could be especially important for financial institutions in light of the Patriot Act's so-called "sleeper provision" that will come to life when a financial institution seeks regulatory approval for expansion plans. The Patriot Act requires federal banking agencies to consider a financial institution's record of combating money laundering when reviewing applications in connection with a bank merger or acquisition.98

What is left of financial privacy after these rules is an open question. It seems as though there is no meaningful financial privacy for a person suspected by a law enforcement official to be a money launderer. Nevertheless, the Treasury Department still officially gives lip service to the idea that citizens enjoy some measure of financial privacy. In testimony before the Senate Committee on Banking, Housing, and Urban Affairs, Kenneth W. Dam, Deputy Secretary of the Treasury, provided an example of the doublethink world we now inhabit when he stated that one of the administration’s primary objectives in implementing the Patriot Act is the protection of consumer privacy.99

---

93. See FinCEN website, http://www.fincen.gov/ (last visited Dec. 15, 2005) (providing access to the form a financial institution to submit their intention to engage in the sharing of information with other financial institutions or associations of financial institutions).
94. Id.
96. Id.
97. Id.
99. The Financial War on Terrorism and the Administration's Implementation of the Anti-Money Laundering Provisions of the USA Patriot Act, Hearings Before the Senate Comm. on Banking, Housing, and Urban Affairs, 107th Cong. (2002) (statement of Kenneth W. Dam, Deputy Secretary, U.S. Dept. of the Treasury), available at http://banking.senate.gov/02_01hrg/012902/dam.htm (last visited Aug. 8, 2005) (noting that although "more than ever law enforcement and the intelligence community must have the ability to obtain and share financial information . . . that need must always be balanced against our fundamental notions of privacy").
III. HOW THE PATRIOT ACT HAS BEEN USED

As I and others have argued elsewhere, it is difficult to show that anti-money laundering laws are effective in preventing criminal activity. The scheme currently in place, however, will be extremely useful in building a routine criminal case against a routine criminal suspect. Now that the process is more of a two way street, the law enforcement community can get the suspect’s financial records more easily. The section 314(a) process enables an investigator to canvass the nation’s financial institutions for potential lead information that might otherwise never be uncovered.

This mechanism will allow investigators to focus quickly on relevant locations and activities. This unprecedented cooperative effort between the financial community and law enforcement permits scattered bits of financial information to be identified, centralized, and evaluated. This innovation is great for law enforcement officials, but it should raise concerns for people who value privacy rights.

The anti-money laundering provisions of Title III of the Patriot Act are not limited in their applicability to terrorism investigations. In one celebrated case, dubbed “Operation G-Sting,” the anti-money laundering provisions of the Patriot Act were used to track the financial transactions of several parties allegedly involved in a scheme in which public officials accepted bribes and sold their votes in order to bend the rules for a Las Vegas strip club. Although the case clearly involved illegal activity, there was not even a whiff of terrorism involved. Nevertheless, the Patriot Act was used to make a case against the participants in a garden variety municipal corruption scheme. Supporters of the Patriot Act defended the use of the law in this context. They noted that nothing in the law limits its application to terrorist investigations, and they are absolutely right.

The use of the anti-money laundering provisions in Operation G-Sting was not illegal, even if members of Congress who voted for the Patriot Act might be surprised that Title III applies to run-of-the-mill criminal activity. The availability of such a powerful tool for routine cases raises legitimate concerns for the defense bar, given the penchant for prosecutors to use allegations of money laundering to bolster their cases. Indeed, prosecutors have used money laundering violations as a

100. See Gouvin, supra note 21, at 989 (arguing that using the money-laundering laws to shut down terrorism is extremely ambitious and may not be feasible); Mariano-Florentino Cuellar, The Tenuous Relationship Between the Fight Against Money Laundering and the Disruption of Criminal Finance, 93 J. CRIM. L. & CRIMINOLOGY 311, 312 (2003) (stating that the fight against money laundering delivers less than it promises).

101. See Steve Friess, Patriot Act Gets Mixed Reviews in Vegas, THE BOSTON GLOBE, Nov. 8, 2003, at A3 (asking if a law allegedly crafted to fight terrorism has been properly used to subpoena financial information in a public corruption case); John M Broder, A New Tale in Legalized Las Vegas Vice, THE N.Y. TIMES, Dec. 15, 2003, at A24 (describing how the FBI used a provision of the Patriot Act to obtain financial records in a Las Vegas public corruption case); and John L. Smith, Corruption Probe Clearly Within Parameters of Patriot Act Foes, LAS VEGAS REV.-J., Nov. 5, 2003, at 1B (stating a similar proposition as the Broder article).

102. See, e.g., Friess, supra note 101, at A3 (quoting Nevada Congressman Jim Gibbons asserting that the Patriot Act was designed not just to counter terrorism, but also to modernize and strengthen the F.B.I.).
device to leverage up the criminal consequences for regulated behavior, creating incentives for the accused to plea bargain.

The poster boy for this problem is a Honduran lobsterman named David Henson McNab. McNab and three associates were convicted of violating the Lacey Act, which prohibits the importation of fish or wildlife caught or sold in violation of U.S. or "any foreign law." A small percentage of the lobsters McNab imported into the United States were allegedly in violation of the lobster size regulations of Honduras and, in addition, the imported lobster was packed in plastic bags instead in cardboard boxes, another alleged violation of Honduran law. Because the proceeds from the sale of the illegal lobster were deposited in banks, McNab was also charged with money laundering. McNab was found guilty of, among other things, sixteen counts of money laundering. He was sentenced to eight years in prison. A petition for writ of certiorari was denied by the United States Supreme Court. The McNab case illustrates how devastating the money laundering laws can be in the hands of the government. We ought to permit this power only when prosecutors and law enforcement agencies are subject to sufficient checks and balances to ensure that abuse of privacy and civil liberties will not occur.

Prior to the passage of the Patriot Act and the promulgation of the regulations implementing it, the only way for a law enforcement agency to get the actual financial records of a suspect was to obtain a subpoena. Today that is still technically true, but because of the regulations implementing section 314(a), law enforcement agencies know with great certainty where they should be looking and, even before they seek a subpoena, they know a great deal about the financial transactions of the subject. Nevertheless, it remains true that section 314(a) is supposed to provide lead information only and is not a substitute for a subpoena or other legal process.

To obtain documents from a financial institution that has reported a match, a law enforcement agency must meet the legal standards that apply to the particular investigative tool that it chooses to use to obtain the documents. Although a grand jury subpoena is the normal mechanism, increasingly, the device used to obtain the records is an administrative subpoena. The due process safeguards for administrative subpoenas are modest at best.

To appreciate how modest, it is worthwhile to contemplate how government requests for information fall into a general hierarchy. The various levels of the hierarchy provide various levels of protection for the party from whom information is sought. In addition, the person from whom the information is sought often has strategies for challenging the request or even avoiding compliance with it. At the

104. United States v. McNab, 331 F.3d 1228, 1234 (11th Cir. 2003).
105. Id. at 1232-33.
highest level of due process protection are search warrants. The issuance of search warrants is governed by the Fourth Amendment, Federal Rule of Criminal Procedure 41, and extensive case law. A search warrant may issue only after a judicial determination that probable cause exists. Once issued, the power to actually use the search warrant is within the exclusive power of a law enforcement officer and attorney for the government. Search warrants go into effect immediately upon issuance. Although the issuance of a search warrant may be challenged, that challenge does not take place until after the warrant has been executed.

The next device for compelling the production of information in the general hierarchy is the subpoena *duces tecum*. Although these subpoenas are issued through a court, the preparation and drafting is actually controlled by the prosecutor’s office. They are issued in the name of the Grand Jury. Subpoenas *duces tecum* can require the production of almost any kind of information. They are governed by Federal Rule of Criminal Procedure 17, but there are virtually no Fourth Amendment protections in connection with the subpoena process. That being said, the effect of a grand jury subpoena is somewhat less dramatic than a search warrant. For example, a grand jury subpoena does not authorize law enforcement agents to enter the subject’s premises to conduct interviews or obtain evidence. The subject of the grand jury subpoena ordinarily will be given some period of time to respond.

Recipients of subpoenas have some avenues available to challenge the request. For example, if compliance with the subpoena would be oppressive or unreasonable, or if it would disclose privileged matters, the court supervising the grand jury may, upon motion, quash or modify the subpoena. In addition, a subpoena may be quashed for failing to identify the materials sought with sufficient clarity and specificity. These procedural safeguards give defendants and others involved in the investigative process some leverage to deal with law enforcement officials, although in practice most requests to quash a subpoena are unsuccessful.

An even less formal method for compelling the production of information is the administrative subpoena issued by a federal or state government agency. An administrative subpoena may be issued without a court order or an independent determination of probable cause (i.e., it may be issued with significantly less justification than a search warrant). Indeed, the touchstone for the issuance of an administrative subpoena is merely that the “information sought is reasonably relevant” to the investigation. The administrative subpoena provides few

---

109. U.S. CONST. amend. IV.
110. FED. R. CRIM. PROC. 41(b).
112. FED. R. CRIM. PROC. 17.
procedural safeguards for the subject of the inquiry. The person receiving the administrative subpoena must respond unless he or she obtains a court order blocking enforcement. The grounds for opposing an administrative subpoena include: whether the administrative agency has statutory authority to issue a subpoena; whether the subpoena seeks privileged or protected material; and whether the subpoena is overbroad and unduly burdensome. In the context of subpoenas seeking financial records as part of a prosecutorial fishing expedition to find evidence that might uncover unknown illegal activities, an administrative subpoena may be challenged on the ground that its purposes are not sufficiently definite. One safeguard provides that an administrative agency cannot enforce its own subpoena. If the subject of the subpoena refuses to comply, the agency must file an action with the court. Unjustified refusal to comply on the part of the subpoena’s recipient, however, could result in the imposition of court sanctions, so usually moving to quash or limit the subpoena is the safer course.

Of course, the law enforcement agency needs a subpoena only if it plans to obtain the actual financial records. Financial records are not subject to a subpoena or search warrant requirement in connection with a section 314 request. The only real check on that administrative power, given that the targets of the section 314 searches cannot be informed that their account information was provided to the requesting law enforcement agencies, is a self-imposed rule from FinCEN. This rule requires federal law enforcement to provide assurances that the request has been subject to appropriate scrutiny at the agency level and that the matter under investigation satisfies FinCEN’s standards for processing a formal section 314(a) inquiry. To document the need for the section 314(a) request, FinCEN requires all requesters to submit a form certifying that the investigation is based on credible evidence of terrorist financing or money laundering. Of course, there are no parties in a credible position to challenge the certification. As noted, the real parties in interest—the individuals whose information is about to be divulged—are not informed, and by law cannot be informed, that the section 314(a) request affecting their accounts has been made. The financial institutions affected cannot afford to challenge every section 314 request, nor will they want to in light of the “good citizen” dynamic discussed earlier where institutions dare not be seen as unsupportive of vigorous anti-money laundering efforts.

In part because of the heavy-handed overreaching of the McNab case, FinCEN

(quotting United States v. Morton Salt Co., 338 U.S. 632, 652 (1950)).

116. See id. at 1418 (holding that where the Office of Thrift Supervision issued an administrative subpoena in part to uncover “other wrongdoing, as yet unknown” the proffered purpose of the subpoena was too indefinite to permit the court to assess whether the information requested met the standard of being “reasonably relevant”).

117. To round out the typology of information seeking devices, the next step in the hierarchy would be informal requests for information. These requests have no real procedural aspect to them. In many cases, however, government investigators simply ask for information on an informal basis and the person from whom the information is requested may or may not comply based on factors such as a willingness to be cooperative. For these informal requests there is no legal basis to compel compliance, but non-legal pressures may make some targets cooperate in order to avoid antagonizing officials.

118. See supra note 93 (stating that financial institutions of which FinCEN makes information requests may not disclose to anyone that FinCEN has requested information).
now requires that the agencies requesting a section 314(a) search determine that the money laundering aspect of the case is significant. In order to guard against inappropriate requests, FinCEN requires documentation showing "the size or impact of the case, the seriousness of the underlying criminal activity, the importance of the case to a major agency program, and any other facts demonstrating its significance." 119 In addition, FinCEN will no longer process a section 314(a) money laundering request in cases where available traditional means of investigation have not been exhausted. 120 These internal procedural changes, if adhered to, will help prevent abuses like those that occurred in the Operation G-Sting and McNab cases. Relying on the agency itself to honor its own procedures is not usually how our system ensures that all citizens receive due process, but it is better than nothing. Yet without the possibility of an adversarial process whereby the affected party can challenge the use of the section 314(a) process, the threat of continued abuse remains very real.

To date, the section 314(a) process has allowed law enforcement agencies to use legal processes to investigate many businesses and organizations, often ostensibly non-profit groups, which may be related to terrorist financing. 121 But the law has also been used far beyond terrorist-related investigations. According to FinCEN, section 314(a) requests have included: a Hawala operation, arms trafficking, alien smuggling, cigarette smuggling, investment fraud, an international criminal network, and drug trafficking. 122

According to the "314(a) Fact Sheet" published by FinCEN, between February 2003 and December 2004, the section 314(a) system processed 367 requests submitted by ten Federal Agencies conducting significant criminal investigations. Of those investigations, 132 cases involved terrorism or terrorist financing, while the remaining 235 cases (almost twice as many as the terror-related cases) involved "money laundering"—which could be almost anything as long as it involves the movement of funds tainted by criminal activity. 123 FinCEN's official tally shows that to date the 314(a) searches have resulted in, among other things, the following: 1,378 new accounts identified, eleven search warrants, 725 grand jury subpoenas, 129 administrative subpoenas, summons or other legal process, nine arrests, and two indictments. 124

From the point of view of the law enforcement community, the section 314(a) process is clearly a success. From the point of view of the individuals whose accounts were accessed, we cannot be so sure. For one thing, there is no way to know whose accounts have been affected and what the consequences of being the

119. FinCEN's 314(a) Fact Sheet, supra note 83.
120. Id.
122. FinCEN's 314(a) Fact Sheet, supra note 83.
123. Id. FinCEN notes that there were 2,599 subjects of interest identified in the investigations and that financial institutions responded with 19,471 total subject matches: 18,550 positive and 921 inconclusive. Id.
124. Id.
subject of a section 314 request have been. One can imagine that in a world where financial institutions are being evaluated by their regulators based in part on how zealously the institution helps to combat money laundering, institutions may begin to treat customers in whom law enforcement agencies show an interest as persona non grata—even if the criminal investigation turns up no wrongdoing. The section 314 process is especially pernicious because customers never know that their account information has been accessed, so they may suffer the consequences of a section 314 request and not be able to link the institution’s actions to its existence.

IV. WHAT’S NEXT?

Proponents of financial privacy need to come to peace with the idea that Title III of the Patriot Act is here to stay and will not go away anytime soon. People who value financial privacy ought to start thinking about ways to ameliorate the loss of privacy brought about by the Patriot Act.

One place to start is to recognize that we have based our due process protections around an adversarial system. We believe people looking out for their own interests is the best safeguard for political and legal rights. In the context of anti-money laundering law, however, there may be something to be said for not giving notice to the people whose account information is being accessed, as the real criminals being investigated may flee. Relying just on FinCEN alone to do the right thing, however, should give a civil libertarian pause. Perhaps as a compromise it would make sense for the law to place an organization outside of FinCEN into the mix to act as a proxy for the real parties in interest.

We could change the law to enable Congress or the courts to play an oversight role to keep FinCEN on the straight and narrow. Judges would be appropriate in this oversight role, as they have to make decisions about investigations of criminal suspects all the time. The section 314 process could be changed to require that FinCEN make periodic reports to a designated judge in order to show that the imposed procedural safeguards are in fact being observed. Similarly, Congress, or an adjunct arm of Congress, such as the General Accounting Office, could provide the oversight necessary to ensure that the good intentions of FinCEN are translated into a process that really does respect suspects’ financial privacy to the maximum degree.

Another procedural change that might bring some solace to those who value financial privacy would be for Congress to implement a true sunset provision for the money laundering provisions of the Patriot Act. Indeed, some proponents of the Patriot Act’s anti-money laundering provisions could maintain that the money laundering provisions were already subject to a “sunset clause.” Yet a closer examination of the so-called sunset provision, section 303,125 reveals that it is not a

---

125. The provision, section 303 of the Patriot Act, states as follows:

IN GENERAL—Effective on and after the first day of fiscal year 2005, the provisions of this title and the amendments made by this title shall terminate if the Congress enacts a joint resolution, the text after the resolving clause of which is as follows: “That provisions of the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001, and the amendments made thereby, shall no longer have the force of law.”
sunset provision at all. As written, the law would have sunset only if it had been repealed. In a true sunset provision, the law ceases to have effect unless it is reauthorized.\textsuperscript{126} But the money laundering provisions of the Patriot Act continued to have effect even after its “sunset” date because Congress did not pass a joint resolution to repeal the law. To call section 303 of the Patriot Act a “sunset” provision is an act of political cynicism of the deepest nature.

In effect what this provision says is that in 2005 Congress could undo this Act by passing an appropriate bill. But of course Congress always has that power—this is no sunset provision at all. The sun will only set if Congress actually resolves to terminate the money laundering provisions. Given the political difficulty of opposing the Patriot Act generally and the money laundering rules in particular, this, not surprisingly, has not happened and will not happen.

Finally, one way to correct some of the possible abuse of the process would be to at least inform customers after the fact, in searches that turn up no suspicious activity, that their records have been the subject of a section 314 request. As discussed above, in the current climate of fear, where financial institutions can be penalized by their regulators for being perceived as uncooperative in the war against terror, there may be incentives for financial institutions to cut off dealings with customers who are merely suspected of being involved in terrorism. Indeed, there may be pressures to engage in ethnic profiling to get rid of customers who are likely to be the subject of section 314(a) requests. Of course, this would be reprehensible, but we must guard against it, as stranger things have happened.

CONCLUSION

The anti-money laundering provisions in Title III of the Patriot Act shift the balance of power toward law enforcement in the long-running debate about how much financial privacy people are entitled to. By making the anti-money laundering scheme a “two way street” in which law enforcement both receives data from financial institutions and can direct financial institutions to report on specific suspects, the Patriot Act gives law enforcement agencies a powerful tool to build cases against both terrorists and run-of-the-mill criminals. The law has already been used in ways that come as a surprise to many people who thought the goal of the legislation was fighting terrorism.

Although FinCEN promises to use the new powers only when law enforcement agencies certify the seriousness of the cases, the lack of adversarial proceedings where the real party in interest can stand up to fight for its position leaves a lot of room for concern. We will never know whether FinCEN does a

\textsuperscript{126} For an example of a true sunset provision, see section 224 of the Patriot Act, which reads as follows:

(a) In General—Except as provided in subsection (b), this title and the amendments made by this title (other than sections 203(a) 203(c), 205, 208, 210, 211, 213, 216, 219, 221, and 222, and the amendments made by those sections) shall cease to have effect on December 31, 2005.

USAPA § 224.
great job or a poor job in respecting financial privacy. The process ought to be amended to provide some degree of oversight that is outside of the internal process FinCEN currently employs.