Privacy Rights v. Anti-Money Laundering Enforcement

Robert S. Pasley

Follow this and additional works at: http://scholarship.law.unc.edu/ncbi
Part of the Banking and Finance Law Commons

Recommended Citation
Available at: http://scholarship.law.unc.edu/ncbi/vol6/iss1/7

This Article is brought to you for free and open access by Carolina Law Scholarship Repository. It has been accepted for inclusion in North Carolina Banking Institute by an authorized administrator of Carolina Law Scholarship Repository. For more information, please contact law_repository@unc.edu.
PRIVACY RIGHTS V. ANTI-MONEY LAUNDERING ENFORCEMENT

ROBERT S. PASLEY

I. INTRODUCTION

There has long been a tension between preserving privacy rights and concerns and enforcing a strong and effective anti-money laundering effort. The legislation in these areas has been plentiful. However, it has also often been complicated and controversial. The court cases interpreting the nature and extent of people's Fourth Amendment privacy rights, as well as the scope and constitutionality of anti-money laundering laws and regulations, have not always been consistent or well reasoned. In addition, because the courts and the legislature have not always agreed on these issues, some legislation has been passed to overturn various court decisions, thus, supplanting common law doctrines with statutory procedures. Finding the right balance—legislatively and judicially—between the two potentially competing interests has been difficult. This is particularly problematic as we implement the latest anti-money laundering statute, the USA Patriot Act, and attempt to improve the security of our country against international terrorism.

As set forth by the Privacy Protection Study Commission, the tension between privacy interests and anti-money laundering efforts represents a long-standing issue: "the balance to be struck

1. Robert S. Pasley is an Assistant Director of the Enforcement and Compliance Division of the Office of the Comptroller of the Currency (OCC). The views expressed in this article do not necessarily represent the views of the OCC.


is an old one; it reflects the tension between individual liberty and social order. The sovereign needs information to maintain order; the individual needs to be able to protect his independence and autonomy should the sovereign overreach."

Our rights and interests in privacy are extremely strong and are anchored in the Constitution. As set forth by Justice Brandeis in his famous dissent:

The makers of our Constitution... conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.

This sentiment was echoed by Judge Field, who later became a Justice of the Supreme Court:

Of all the rights of the citizen, few are of greater importance or more essential to his peace and happiness than the right of personal security, and that involves, not merely protection of his person from assault, but exemption of his private affairs, books, and papers from the inspection and scrutiny of others. Without the enjoyment of this right, all other rights would lose half of their value.

While privacy interests are highly valued, so are the interests of being safe and secure from drug trafficking, money laundering and terrorism. As found by the Congressional Office of Technology Assessment (OTA):

Money Laundering is one of the most critical problems facing law enforcement today.

International crime probably cannot be controlled or reduced unless criminal organizations can be deprived of their illegal proceeds. ... Some minimum level of social and economic costs may therefore be acceptable in order to strengthen law enforcement against the threat posed by financial crime.

In a very insightful comment, relevant to today's post September 11th concerns, the OTA also noted that:

Terrorists, as well as drug traffickers and other criminal organizations, need to launder money. It takes money for weapons and explosives. It takes money to get terrorists to their targets, and then into hiding. Continuing subversive organizations also need money for maintaining networks, and for the support and protection of active members, their dependents, and their survivors.

The theme of playing off our privacy rights and interests against those of anti-money laundering is recurring. As quoted in the American Banker in 1989, then Attorney General Richard Thornburgh told a group of bankers and lawyers: "Banks must play a key role in fighting the nation's drug problem even at the risk of sacrificing customer privacy. ... The most vulnerable point for any drug operation is at the doorway to the bank."


8. Id. at 121.

In addition, news reports point out various mood swings within the country on the issue:

It was just last spring that the public’s wrath over the proposed “Know Your Customer” (KYC) regulations made the headlines and caused the banking agencies to withdraw their long-awaited proposal. . . . But this fall, as Congress held hearings about alleged Russian money laundering, the KYC proposal has largely been forgotten. . . . Consumer privacy is taking a back seat to outrage over the use of U.S. financial institutions to launder money. The irony is not lost on the banking industry.  

More recently, another commentator similarly noted:

The terrorist attacks on America have substantially changed the issues surrounding financial privacy. Prior to Sept. 11, privacy advocates were pushing hard for assurances that banks are respecting the confidentiality of personal financial information. Now those advocates are taking a back seat to those who say government agencies and law enforcement officials need greater access to financial information to shore up our national security. . . . Perhaps the sacrifice is small considering we are a nation at war. . . . Ultimately, bankers will always have to perform a delicate balancing act which respects the privacy of customers yet supports the law enforcement communities’ efforts to maintain national security.  

Likewise, a commentator recently claimed: “In the battle of security versus liberty, security is now winning. . . . Civil liberties


will no longer be able to stand in the way of the war on terrorism."\textsuperscript{12}

It is wrong, however, to view this delicate balancing issue in terms of winning or losing, in terms of who is in the driver's seat and who is "taking a back seat." Assuming the proper balance can be reached—and, empirically, there should be a place where there is a proper balance—that balance should not fluctuate based only on external events. As the Supreme Court noted: "If [the war on drugs] is to be fought, those who fight it must respect the rights of individuals....\textsuperscript{13} Similarly, in a case from another war, World War II, Justice Murphy said in a dissent:

At a time when the nation is called upon to give freely of life and treasure to defend and preserve the institutions of democracy and freedom, we should not permit any of the essentials of freedom to lose vitality through legal interpretations that are restrictive and inadequate for the period in which we live.\textsuperscript{14}

This article addresses the importance of financial privacy and anti-money laundering enforcement and the tension between the two. After first providing a general analysis of the cases interpreting privacy rights under the Constitution,\textsuperscript{15} this article sets forth a more specific examination of the cases interpreting financial privacy rights under the Fourth Amendment.\textsuperscript{16} Next, this article analyzes the case law that has interpreted banks' liability for alleged violations of financial privacy and the Bank Secrecy Act (BSA).\textsuperscript{17} With this background, this article then addresses the constitutionality of the BSA and its requirements.\textsuperscript{18} Finally, this article examines the USA Patriot Act and the Right to Financial Privacy Act in light of our current need for supporting strong anti-


\textsuperscript{15} \textit{See infra} notes 20-89 and accompanying text.

\textsuperscript{16} \textit{See infra} notes 90-126 and accompanying text.

\textsuperscript{17} \textit{See infra} notes 127-251 and accompanying text.

\textsuperscript{18} \textit{See infra} notes 252-325 and accompanying text.
money laundering efforts without losing sight of the importance of financial privacy.¹⁹

II. IMPORTANCE OF FINANCIAL PRIVACY

Americans value their financial privacy almost more than any other area. The concern over financial privacy is well-founded since an analysis of a person's bank account can reveal much about the individual. As one commentator noted:

Financial information has become such an important concern because an individual's banking transactions directly reflect that individual's lifestyle, personal interests, and political beliefs. With access to an individual's financial records, interested parties can easily determine the groups and associations to which the individual belongs (e.g., through membership dues or contributions) and the social causes the individual supports (e.g., through contributions). With access to banking records, interested parties can identify the books and publications an individual buys (e.g., through subscription payments or receipts) and the material items an individual purchases (e.g., through receipts or credit charges). Prying eyes with access to bank records can even identify the political party and causes supported by the individual (e.g., through contributions to an election campaign or to a lobbying group).

Financial records further allow interested observers to recreate a financial "snapshot" of the individual. Stocks and bonds, insurance, real estate, retirement funds, cars, homes, personal property, loans, mortgages, alimony, and child support are all discoverable from financial records. Credit card records can trace individuals in their every physical movement—to different countries, states, or cities,

¹⁹. See infra notes 326-422 and accompanying text.
and even to restaurants, to stores, to airline travel, and to hotels.\textsuperscript{20}

These ideas are echoed in court cases:

For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account. In the course of such dealings, a depositor reveals many aspects of his personal affairs, opinions, habits and associations. Indeed, the totality of bank records provides a virtual current biography.\textsuperscript{21}

As Justice Douglas said in a dissent: "the banking transactions of an individual give a fairly accurate account of his religion, ideology, opinions, and interests.\ldots"\textsuperscript{22} This was later colorfully reiterated by a lower court: "the message of Mr. Justice Douglas in \[the] Shultz \[case\] is clear: If it is true that a man is known by the company he keeps, then his soul is almost laid bare to the examiner of his checking account."\textsuperscript{23}

The right to privacy has also been frequently recognized and upheld by the courts:

That there is such a thing as a constitutionally protected "right of privacy" has been recognized by the Supreme Court in such cases as Griswold v. Connecticut; Katz v. United States; and most recently in United States v. United States District Court.\textsuperscript{24}

\textsuperscript{20} Kleiman, \textit{supra} note 2, at 1176.

\textsuperscript{21} Burrows v. Superior Court of San Bernardino County, 529 P.2d 590, 596 (Cal. 1975).


Similarly, there is a long list of statutes designed to protect the privacy rights and interests of individuals.\textsuperscript{25}

However, people’s privacy rights must be balanced against the need for physical security and effective law enforcement, in general, and anti-money laundering enforcement specifically. Anyone who has flown or has even entered a government building since September 11, 2001 knows how thorough the search for weapons can be and understands the reasons for it. It is now common for airlines, through random, enhanced searches, to examine your carry-on bags and to remove all of your papers from your briefcase. As always, whenever you pass through Customs, your person and luggage can be thoroughly searched, and you can be questioned as to your plans and travel status. And, as noted by the Supreme Court, in order to support the needs of law enforcement, providing blood samples, handwriting exemplars and voice exemplars is not viewed as an unconstitutional invasion of privacy.\textsuperscript{26} The Court has even ruled that random highway stops, without any warrant, suspicion or provocation, in order to check sobriety or immigration status, are not unconstitutional invasions of privacy.\textsuperscript{27} Given these competing interests between privacy and law enforcement (and, in particular, anti-money laundering enforcement), the overriding issue is where the balance should be.

III. IMPORTANCE OF ANTI-MONEY LAUNDERING ENFORCEMENT

After the tragic events of September 11, 2001, there can be no doubt that there is a need for strong anti-money laundering enforcement. As noted even years before this terrorist attack, “[w]orld stability is increasingly threatened by sophisticated criminal organizations and their creative implementation of money


\textsuperscript{26} Fisher v. United States, 425 U.S. 391, 408 (1976).

laundering schemes. This fact was noted again recently by the Secretary of the Treasury: "The threat that terrorism poses to the world financial system demands from us an expanded effort to combat the financing of terrorism and terrorist acts."

Similarly, the need to employ strong anti-money laundering enforcement efforts was set forth by Under Secretary of the Treasury Gurule:

Let me begin by saying that criminal acts of violence, such as the horrific terrorist attacks of September 11th, need more than just cunning leadership and dedicated followers to be successful. Such undertakings also require extensive financial funding as well. Although the complexities of money laundering have long been associated with concealing the true nature of proceeds generated from the drug cartels, the tragedies of September 11th also underscore the need for aggressive and vigilant anti-money laundering efforts which target the movement of funds into this country for the purpose of criminal activity—especially funds earmarked for terror.

As explained by Deputy Secretary of the Treasury Dam in recent testimony before the Senate Banking Committee:

Mr. Chairman, we are engaged in a long-term battle against illegal abuse of the financial system. Whether it is terrorist financing or classic narcotics money laundering, we need to take every measure possible to combat the evil deeds that soil our


financial system and pose a real threat to our security.\textsuperscript{31}

Even prior to the events of September 11th, the threat and impact of money laundering was clear. In a report from the United States Department of State, there is the following excellent explanation of the concerns and consequences associated with money laundering:

Money laundering is necessitated by the requirement for criminals, be they drug traffickers, organized criminals, terrorists, arms traffickers, blackmailers, or credit card swindlers, to disguise the origin of their criminal money so that they can use it more easily.

Money laundering has devastating social consequences and is a threat to national security. It provides the fuel for drug dealers, terrorists, illegal arms dealers, corrupt public officials and other criminals to operate and expand their criminal enterprises.

Unchecked, money laundering can erode the integrity of a nation's financial institutions.

Ultimately, this laundered money flows into global financial systems where it could undermine national economies and currencies. Money laundering is thus not only a law enforcement problem but poses a serious national and international security threat as well.

Money launderers also negatively impact jurisdictions by reducing tax revenues through

underground economies, competing unfairly with legitimate businesses, damaging financial systems, and disrupting economic development. . . . Fighting money launderers not only reduces financial crime; it also deprives criminals and terrorists of the means to commit other serious crimes.32

Many of these thoughts and concerns were the foundation of the Department of Treasury's and the Department of Justice's joint 2001 National Money Laundering Strategy:

The 2001 [National Money Laundering] Strategy recognizes that money laundering is an integral component of large-scale criminal enterprises. Drug trafficking, firearms smuggling, international bank and securities frauds, bribery, intellectual property theft, and other specified unlawful activity generate illicit proceeds that criminals must conceal. . . . Once criminals successfully disguise their illicit proceeds, they then can reinvest them in their criminal organizations, expand their operations, and profit from their crimes.33

It should also be noted that the economic costs alone of money laundering have consistently been estimated in phenomenal amounts:

In 1996, the United Nations estimated that US $1 billion daily was involved in money laundering. The Commercial Crime Bureau of the International Chamber of Commerce believe this figure to be greatly understated.34

34. INTERNATIONAL CHAMBER OF COMMERCE, GUIDE TO THE PREVENTION OF MONEY LAUNDERING, JOURNAL OF COMMERCE 4 (June, 1993) (on file with the N.C. Banking Institute).
Despite increasing international attention and stronger anti-money laundering controls, some current estimates are that $500 billion to $1 trillion in criminal proceeds are laundered through banks worldwide each year, with about half of that amount moved through United States banks.\textsuperscript{35}

For example, former IMF Managing Director Michael Camdessus estimated the global volume of laundering at between two and five percent of the world's gross domestic product, a range which encompasses sums between $600 billion and $1.8 trillion.\textsuperscript{36}

With regard to terrorism alone, the amount of money involved is surprisingly large. As Deputy Secretary of the Treasury Dam testified: "Since September 11th, the United States and other countries have frozen more than $80 million in terrorist-related assets."\textsuperscript{37}

As evident from these concerns, problems, and consequences related to it, money laundering is a very serious matter that needs to be addressed through strong measures. To demonstrate how enforcement efforts interact with individual privacy rights and concerns, it is useful to explore the case law pertaining to privacy rights in general and privacy rights as they specifically relate to financial records.


IV. CASES INTERPRETING PRIVACY RIGHTS UNDER THE FOURTH AMENDMENT

The cases interpreting the scope of an individual's privacy rights under the Fourth Amendment have been varied and even contradictory.

In a seminal Fourth Amendment case that came before the Supreme Court, *Olmstead v. United States*, the plaintiffs complained that the police had unlawfully and unconstitutionally wiretapped their phones. In fact, the police had wiretapped eight phones over a period of five months. The government acknowledged that it had not obtained a search warrant for the wiretapping and that the wiretapping was illegal under state law, but contended that the illegally obtained evidence should be admitted anyway. The Court agreed.

The case involved "a conspiracy to violate the National Prohibition Act by unlawfully possessing, transporting... importing [and selling] intoxicating liquors." It was a conspiracy of "amazing magnitude" that had "two seagoing vessels" and employed over 50 people, including "executives, salesmen, deliverymen, dispatchers, scouts, bookkeepers, collectors and an attorney." The enterprise moved 200 cases of liquor per day and had annual sales in excess of $2 million.

It does not appear, however, that the Court was concerned about the size or seriousness of the conspiracy. Rather, the Court simply focused on an overly restrictive interpretation of the Fourth Amendment premised primarily on the historical tests of whether a particular place or area had been invaded. The wiretaps, which apparently provided the necessary evidence for the convictions, did not involve a physical entry into the plaintiffs' houses or offices. Instead, as the Court emphasized, the wiretaps were made

39. *Id.* at 455.
40. *Id.* at 471 (Brandeis, J., dissenting).
41. *Id.* at 466, 468.
42. *Id.* at 469.
43. *Id.* at 455.
44. *Olmstead*, 277 U.S. at 455-56.
45. *Id.* at 456.
46. *Id.*
47. *Id.* at 461-65.
"in the basement of large office buildings and along the streets near the houses."\(^{48}\) According to the Court, the "well known historical purpose of the Fourth Amendment ... was to prevent the use of governmental force to search a man's house, his person, his papers and his effects; and to prevent their seizure against his will."\(^{49}\) In this case, according to the Court, there was no entry,\(^{50}\) there was no trespass,\(^{51}\) there was no searching,\(^{52}\) and there was no seizure.\(^{53}\) In addition, the Court was struck by the fact that the "evidence was secured by the use of the sense of hearing and that only."\(^{54}\)

The Court, in upholding the Government's illegal wiretapping, held that: "the language of the Amendment can not be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office any more than are the highways along which they are stretched."\(^{55}\)

Given the fact that the Government had not searched the plaintiffs' "person, house, papers or effects," there was no unconstitutional search and seizure.\(^{56}\)

This case, decided on a 5-4 basis, motivated Justice Brandeis to deliver a scathing and memorable dissent. He emphasized the fact that the police had wiretapped eight telephones over a five month period, and that, in installing the wiretaps, the police had not only committed misdemeanors, but also had caused an employee of the phone company to do so as well.\(^{57}\) Thus, he concluded his dissent with the following admonition:

\(^{48}\) *Id.* at 457.

\(^{49}\) *Id.* at 463.

\(^{50}\) *Olmstead*, 277 U.S. at 464.

\(^{51}\) *Id.* at 457.

\(^{52}\) *Id.* at 464.

\(^{53}\) *Id.*

\(^{54}\) *Id.*

\(^{55}\) *Id.* at 465.

\(^{56}\) *Olmstead*, 277 U.S. at 465. The fact that the wiretapping was also illegal under state law was, according to the Court, not a "valid objection" to its admissibility. *Id.* at 466-67.

\(^{57}\) *Id.* at 471, 479-80 (Brandeis, J., dissenting).
If the Government becomes a lawbreaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy. To declare that in the administration of the criminal law the end justifies the means—to declare that the Government may commit crimes in order to secure the conviction of a private criminal—would bring terrible retribution.\textsuperscript{58}

During the course of his dissent, Brandeis correctly noted that it was immaterial where the physical connection of the wiretapping occurred;\textsuperscript{59} thus undermining the basic tenet of the majority decision. Citing to an old English case, he explained:

It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property, where that right has never been forfeited by his conviction of some public offense ....\textsuperscript{60}

By analogy, Brandeis pointed out the fact that a letter which is mailed through the postal system is protected by the Fourth Amendment even though it travels outside of the house.\textsuperscript{61} He reasoned that there should be "no difference between the sealed letter and the private telephone message."\textsuperscript{62} In quoting the lower court decision, Brandeis reiterated that: "true the one is visible, the other invisible; the one is tangible, the other intangible; the one is sealed and the other unsealed, but these are distinctions without a difference."\textsuperscript{63}

He went on to note that wiretapping a phone was actually far more invasive than opening a letter, because the former affects

\begin{itemize}
\item \textsuperscript{58} Id. at 485.
\item \textsuperscript{59} Id. at 479.
\item \textsuperscript{60} Id. at 474-75 (citing Entick v. Carrington, 19 Howell's State Trials, 1030, 1066).
\item \textsuperscript{61} Id. at 475 (citing Ex parte Jackson, 99 U.S. 727 (1877)).
\item \textsuperscript{62} Olmstead, 277 U.S. at 475.
\item \textsuperscript{63} Id.
\end{itemize}
all calls and all parties to the call.\footnote{Id. at 475-76.} Bothered by this intrusiveness, Brandeis speculated that:

The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. 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.\footnote{Id. at 474.}

While this insight into the possible future has not come to pass, there are, obviously, many things that go on within a house that can be revealed, such as what is sent or ordered via computer, what is ordered via pay TV, and even what is communicated via on-line banking.

Similarly to \textit{Olmstead}, in \textit{Goldman v. United States},\footnote{Goldman v. United States, 316 U.S. 129 (1942).} the Court's decision set forth a similarly restrictive view of people's privacy rights under the Fourth Amendment.\footnote{Id. at 135-36.} In this case, the Petitioners were indicted for conspiracy to violate the Bankruptcy Act.\footnote{Id. at 130.} The conspiracy involved undervaluing the assets of the person in bankruptcy, selling the assets at market value, and keeping the difference.\footnote{Id. at 130-31.} The plan was devised by two attorneys, Goldman and Shulman, and was proposed to a third attorney, who ostensibly agreed to the plan, but, in fact, cooperated with the authorities from the outset.\footnote{Id.} In an effort to build a case against the first two attorneys, a meeting in Shulman's office was arranged between all three attorneys.\footnote{Id. at 131.} With the help of a building superintendent, the federal agents on the case gained access to Shulman's office and planted a listening device.\footnote{Goldman, 316 U.S. at 131.} However, when the time came for the meeting, the planted listening device did not
work and the agents resorted to using a sensitive listening device by which they could overhear the lawyers' conversation from an adjoining office.\textsuperscript{73}

The petitioners, in support of their motion to suppress the evidence, tried to distinguish \textit{Olmstead} by arguing that their conversation did not go outside of the room.\textsuperscript{74} In rejecting this Fourth Amendment argument, the Court, in another 5-4 decision, reasoned as follows:

It is urged that where, as in the present case, one talks in his own office, and intends his conversation to be confined within the four walls of the room, he does not intend his voice shall go beyond those walls and it is not to be assumed he takes the risk of someone's use of a delicate detector in the next room. We think, however, the distinction is too nice for practical application of the Constitutional guarantee, and no reasonable or logical distinction can be drawn between what federal agents did in the present case and state officers did in the \textit{Olmstead} case.\textsuperscript{75}

It would appear, however, that it was the Court's own "nice" distinctions in \textit{Olmstead} and \textit{Goldman} that disturbed the dissent:

There was no physical entry in this case. But the search of one's home or office no longer requires physical entry, for science has brought forth far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forebears and which inspired the Fourth Amendment.\textsuperscript{76}

What is curious about \textit{Goldman} is not just the Court's artificial and strict interpretation of the Fourth Amendment, but also the fact that there was, in fact, a "physical entry in this case."

\begin{footnotes}
\item[73.] \textit{Id.} at 131-32.
\item[74.] \textit{Id.} at 135.
\item[75.] \textit{Id.}
\item[76.] \textit{Id.} at 139 (Murphy, J., dissenting).
\end{footnotes}
The only trouble was that that process failed.\textsuperscript{77} If the Government had not been forced to resort to "Plan B" and use a sensitive listening device placed on the wall of the adjoining office,\textsuperscript{78} there probably would have been no question as to the existence of a violation of the Fourth Amendment.

In any event, in the next major Fourth Amendment privacy case, the Supreme Court overturned its earlier decisions in the \textit{Olmstead} and \textit{Goldman} cases.\textsuperscript{79} In this case, \textit{Katz v. United States}, the authorities had placed a wiretap in an outside public pay telephone booth.\textsuperscript{80} The government, in trying to defend the warrantless search, stressed - apparently with a straight face - "the fact that the telephone booth from which the petitioner made his calls was constructed partly of glass, so that he was as visible after he entered it as he would have been if he had remained outside."\textsuperscript{81} However, as the Court correctly pointed out: "[what the Petitioner] sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen."\textsuperscript{82}

In rejecting the \textit{Olmstead} and \textit{Goldman} restrictive interpretation of the Fourth Amendment that was focused on whether there had been a physical entry, the Court in \textit{Katz} established a new doctrine that the Fourth Amendment "protects people, not places."\textsuperscript{83} Even though, as the Court found, the agents in \textit{Katz} had acted with restraint, such self-imposed restraint could not take the place of a prior judicial review of the action in order to protect people's rights under the Fourth Amendment:

It is apparent that the agents in this case acted with restraint. Yet the inescapable fact is that this

\textsuperscript{77. Id. at 131.}
\textsuperscript{78. Goldman, 316 U.S. at 131.}
\textsuperscript{80. Id. at 348.}
\textsuperscript{81. Id. at 352.}
\textsuperscript{82. Id.}
\textsuperscript{83. Id. at 351. However, it should be noted that the Court, while making this pronouncement, nonetheless stressed the importance of the place: "One who occupies [a public pay telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world." Id. at 352.}
restraint was imposed by the agents themselves, not by a judicial officer. They were not required, before commencing the search, to present their estimate of probable cause for detached scrutiny by a neutral magistrate. They were not compelled, during the conduct of the search itself, to observe precise limits established in advance by a specific court order. Nor were they directed, after the search had been completed, to notify the authorizing magistrate in detail of all that had been seized. In the absence of such safeguards, this Court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end.  

Following the reasoning in *Katz*, the Court in *Mancusi v. DeForte* ruled that an officer in a union had a "reasonable expectation of freedom from governmental intrusion" and that a warrantless search of his office on the premises of the union was protected. Many other cases have also cited favorably to *Katz*, including such famous decisions as *Bivens v. Six Unknown Named Agents of the Federal Bureau of Narcotics* (specifically echoing the fact that, pursuant to *Katz*, "the Fourth Amendment is not tied to the niceties of local trespass laws"), and *Roe v. Wade*. This line of cases clearly established a right to privacy under the Fourth Amendment.

V. CASES INTERPRETING FINANCIAL PRIVACY RIGHTS UNDER THE FOURTH AMENDMENT

Similar to the cases interpreting the scope of Fourth Amendment privacy rights in general, the cases analyzing the rights of banking customers and the extent of their financial

---

84. Id. at 356-57.
86. Id. at 368, 372.
87. 403 U.S. 388 (1971).
88. Id. at 393-94.
privacy protections have fluctuated on this controversial issue. Unlike the general privacy rights cases, though, those dealing with financial privacy eventually came to a different result.\textsuperscript{90}

In \textit{Fisher},\textsuperscript{91} the Supreme Court upheld the constitutionality of a summons requiring an attorney to produce work papers that had been created by his clients' accountant and that had been delivered by the clients to the attorney.\textsuperscript{92} In reviewing the applicability of the Fourth and Fifth Amendments to the facts of the case, the Court noted that "[i]t is true that the Court has often stated that one of the several purposes served by the constitutional privilege against compelled testimonial self-incrimination is that of protecting personal privacy."\textsuperscript{93} However, the Court further noted that "[i]t is also clear that the Fifth Amendment does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a \textit{testimonial} communication that is incriminating."\textsuperscript{94}

In upholding the forced production of an accountant's work papers that were not created by the clients, that were not in the clients' possession, and that were testimonial in nature, the Court's decision was not remarkable.\textsuperscript{95} However, in his concurring opinion, Justice Brennan provided an interesting, but inconclusive, discussion of the privacy of financial records:

Nonbusiness economic records in the possession of an individual, such as cancelled checks or tax records, would also seem to be protected. They may provide clear insights into a person's total lifestyle. They are, however, like business records and the papers involved in these cases, frequently, though not always, disclosed to other parties; and disclosure, in proper cases, may foreclose reliance upon the privilege.\textsuperscript{96}

\textsuperscript{92} Id. at 394. It appears that there may have been some effort on the part of the lawyer and his clients to hide the documents in question. \textit{Id}.
\textsuperscript{93} Id. at 399.
\textsuperscript{94} Id. at 408 (emphasis in the original).
\textsuperscript{96} Fisher, 425 U.S. 391, 427 (1976).
It is difficult to determine from this quote where the Court, or even Brennan, was going. The quote is sprinkled too much with phrases such as “seem to be protected” and “may foreclose reliance upon the privilege” to provide any clear guidance. However, the direction of the Court in this area was resolved—at least for the time—by its decision in *United States v. Miller,* which was handed down on the same day as *Fisher.*

In *Miller,* the Court ruled directly on the issue of what financial confidentiality a bank customer could expect. In that case, a fire had broken out in a warehouse being rented by Mr. Miller. The responding firemen and sheriff department found a “7,500 gallon-capacity distillery, 175 gallons of non-tax paid whiskey, and related paraphernalia.”

In the course of investigating the matter further, the Alcohol, Tobacco and Firearms Bureau of the U.S. Treasury Department issued a defective subpoena to Mr. Miller’s banks, which complied with the subpoena. Mr. Miller was subsequently convicted of “possessing an unregistered still, carrying on the business of a distiller without giving bond and with intent to defraud the Government of whiskey tax, possessing 175 gallons of whiskey upon which no taxes had been paid, and conspiring to defraud the United States of tax revenues.” Mr. Miller moved to suppress the banking records, which apparently supported the tax charges.

In ruling that the district court properly denied the motion to suppress, the Court held that the “respondent had no protectable Fourth Amendment interest in the subpoenaed documents.” In relying on an earlier case (and apparently ignoring the more recent *Katz* case that held that even a restrained search that involved no “entry” was not permissible under the Fourth Amendment if it were not sanctioned in advance by a court), the Court seemed to hark back to the *Olmstead* and

---

98. *Id.* at 437.
99. *Id.* at 437-39. The subpoena was signed by a United States Attorney, but not by a court. *Id.*
100. *Id.* at 436.
101. *Id.*
102. *Id.* at 437.
Goldman line of cases, which required an "intrusion" before finding that the Fourth Amendment is triggered:

In *Hoffa v. United States*, 385 U.S. 293, 301-302 (1966), the Court said 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."  \(^{104}\)

The Court further held that the customer's bank documents were neither private nor confidential and were not protected by the Fourth Amendment:

On their face, the documents subpoenaed here are not respondent's "private papers"... respondent can assert neither ownership nor possession. Instead, these are the business records of the banks. Even if we direct our attention to the original checks and deposit slips, rather than to the microfilm copies actually viewed and obtained by means of the subpoena, we perceive no legitimate "expectation of privacy" in their contents. The checks are not confidential communications but negotiable instruments to be used in commercial transactions. All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business. The lack of any legitimate expectation of privacy concerning the information kept in bank records was assumed by Congress in enacting the Bank Secrecy Act, the expressed purpose of which is to require records to

---

104. *Miller*, 425 U.S. 435, 440 (1976). It is curious that the majority decision did not even reference the *Katz* case at this point in the case. Subsequently, the Court "distinguished" away the *Katz* case by simply holding that there is no "legitimate 'expectation of privacy'" in the bank records. *Id.* at 442.
be maintained because they "have a high degree of usefulness in criminal, tax, and regulatory investigations and proceedings."\textsuperscript{105}

Justice Brennan, who filed the ambiguous concurring opinion in \textit{Fisher},\textsuperscript{105} as set forth above, issued a strong dissent in \textit{Miller}.	extsuperscript{107} In his dissent, he relied, in part, on the fact that the California Constitution had a provision that was virtually identical to the language of the Fourth Amendment\textsuperscript{106} that had been interpreted, in \textit{Burrows},\textsuperscript{109} to protect bank records:

The California Supreme Court held that the accused had a reasonable expectation of privacy in his bank statements and records, that the voluntary relinquishment of such records by the bank at the request of the sheriff and prosecutor did not constitute a valid consent by the accused, and that the acquisition by officers of the records therefore was the result of an illegal search and seizure. In my view the same conclusion, for the reasons stated by the California Supreme Court, is compelled in this case under the practically identical phrasing of the Fourth Amendment.\textsuperscript{110}

The majority in \textit{Miller} attempted to distinguish \textit{Burrows} by noting that there was no subpoena in that case and that the bank had provided the records voluntarily:

This case differs from \textit{Burrows v. Superior Court}, \textsc{13 Cal. 3d} 238, 529 P.2d 590 (1974), relied on by Mr. Justice Brennan in dissent, in that the bank records of respondent's accounts were furnished in response

\textsuperscript{105} \textit{Id.} at 440-43.
\textsuperscript{107} \textit{Miller}, 425 U.S. at 447-55.
\textsuperscript{108} \textit{Id.} at 447. The only difference between the two provisions is that the California Constitution says "unreasonable seizures and searches" and the Fourth Amendment, of course, says "unreasonable searches and seizures." \textit{Id.}
\textsuperscript{109} \textit{Burrows v. Superior Court of San Bernardino County}, \textsc{529 P.2d} 590 (Cal. 1975).
\textsuperscript{110} \textit{Miller}, 425 U.S. at 448.
to "compulsion by legal process" in the form of subpoenas *duces tecum*. The court in Burrows found it "significant... that the bank [in that case] provided the statements to the police in response to an informal oral request for information."\textsuperscript{111}

This is all well and good, except for the fact that the subpoena issued in *Miller* was, by all accounts, defective and that the bank, from a legal perspective, had also voluntarily handed over the documents.\textsuperscript{112}

In *Burrows*, a lawyer was suspected of having misappropriated the funds of a client.\textsuperscript{113} The detective on the case had contacted several banks and, without a warrant, had obtained copies of the lawyer's bank statements.\textsuperscript{114} In ruling that this was inappropriate, the court held that:

A bank customer's reasonable expectation is that, absent compulsion by legal process, the matters he reveals to the bank will be utilized by the bank only for internal banking purposes.\ldots Instead, it is argued [by the People], banks have an independent interest in voluntarily cooperating with law enforcement officers because financial institutions desire to foster a favorable public image, and like any good citizen, to assist in the detection of crime. However laudable these motives may be, we are not here concerned with the conduct or reputation of

\textsuperscript{111} *Id.* at 445 n.7.

\textsuperscript{112} *Id.* at 439 ("The subpoenas issued here were found not to constitute adequate 'legal process.' The fact that the bank officers cooperated voluntarily \ldots"); *id.* at 450 (Brennan, J. dissenting) (citing the *Burrows* case description of the lower court *Miller* decision).

The circuit court... held that the defendant's rights under the Fourth Amendment were violated by the search because the subpoena was issued by the United States Attorney rather than by a court or grand jury, and the bank's voluntary compliance with the subpoena was irrelevant since it was the depositor's right to privacy which was threatened by the disclosure.

*Id.* (Brennan, J. dissenting).

\textsuperscript{113} *Burrows*, 529 P.2d at 591.

\textsuperscript{114} *Id.*
banks, but with whether the police violated petitioner's rights by obtaining from banks, without legal process, documents in which petitioner had a reasonable expectation of privacy.115

To permit a police officer access to these records merely upon his request, without any judicial control as to relevancy or other traditional requirements of legal process ... opens the door to a vast and unlimited range of very real abuses of police power.

Cases are legion that condemn violent searches and invasions of an individual's right to the privacy of his dwelling. The imposition upon privacy, although perhaps not so dramatic, may be equally devastating when other methods are employed.116

The argument advanced by the People in *Burrows* that there was no search and seizure because the "bank voluntarily provided the statements to the police, and the bank rather than the police conducted the search of its records..." fell on deaf ears.117

Interestingly, the *Burrows* court relied on the Fifth Circuit's decision in *Miller* before that case was overturned by the Supreme Court.118 In addition, contrary to the Supreme Court decision in *Miller* to the effect that there was "no legitimate 'expectation of privacy' in bank records,"119 in part due to the passage of the Bank Secrecy Act (BSA),120 the *Burrows* court held that the BSA did not conflict with a holding requiring the issuance of a subpoena:

> In *California Bankers Association v. Shultz*, [an] association of bankers, a bank, and some of its

---

115. *Id.* at 593.
116. *Id.* at 596.
117. *Id.* at 595.
118. *Id.* at 594.
customers challenged the validity of the Bank Secrecy Act of 1970. . . . The United States Supreme Court held, in a six-three decision, that the bank’s rights under the Fourth Amendment were not abridged by the regulation. . . . Miller [the Fifth Circuit’s decision] holds that Shultz may not be interpreted as “proclaiming open season on personal bank records” or as permitting the government to circumvent the Fourth Amendment by first requiring banks to copy their depositors’ checks and then calling upon the banks to allow inspection of those copies without appropriate legal process.\textsuperscript{121}

As noted, one of the basic underpinnings of Miller was its interpretation of the privacy effect of the BSA in holding that, because Congress, through the Act, required banks to keep certain records, there could be no expectation of privacy.\textsuperscript{122} Congress disagreed and responded to this non sequitur by passing the Right to Financial Privacy Act of 1978 (RFPA).\textsuperscript{123} As set forth in the House Report on the legislation:

The [RFPA] is a congressional response to the Supreme Court decision in the United States v. Miller which held that a customer of a financial institution has no standing under the Constitution to contest Government access of financial records. The Court did not acknowledge the sensitive nature

\textsuperscript{121} Burrows v. Superior Court of San Bernardino County, 529 P.2d 590, 595-96 (Cal. 1975).
\textsuperscript{122} Miller, 425 U.S. at 442-43.

The lack of any legitimate expectation of privacy concerning the information kept in bank records was assumed by Congress in enacting the Bank Secrecy Act, the expressed purpose of which is to require records to be maintained because they “have a high degree of usefulness in criminal, tax, and regulatory investigations and proceedings.”

\textit{Id.}

of these records, and instead decided that since the records are the "property" of the financial institution, the customer has no constitutionally recognizable privacy interest in them.

Nevertheless, while the Supreme Court found no constitutional right of privacy in financial records, it is clear that Congress may provide protection of individual rights beyond that afforded in the Constitution.\textsuperscript{124}

Once the RFPA was passed, it more or less controlled the issue of when and how financial records could be disseminated to the federal government. As a result, there are relatively few other cases that have reviewed this topic. However, given the fact that \textit{Miller} went against the lower court precedent,\textsuperscript{125} that it could be viewed as being contrary to \textit{Katz}, that it relied on a flawed interpretation of \textit{Burrows},\textsuperscript{126} and that Congress so strongly disagreed with the outcome, one has to wonder if \textit{Miller} would have stayed good law if the RFPA had not been passed to statutorily occupy the area. Regardless, the RFPA, as discussed below, has brought some certainty to the issue of when and how a bank can hand records over to law enforcement authorities.

\textbf{VI. Cases Interpreting Banks' Liability for Alleged Violations of Financial Privacy and the BSA Safe Harbor}

While the cases mentioned above discuss privacy rights under the Fourth Amendment and, specifically, financial privacy, it is important to also explore the historic liability on the part of a bank that discloses its customers' account information and arguably violates the customers' privacy. The first two cases deal with a bank's disclosure to a customer's employer, while the remaining pertain to disclosures to law enforcement authorities.

\begin{itemize}
  \item \textsuperscript{124} \textit{Id.}
  \item \textsuperscript{125} United States v. \textit{Miller}, 500 F.2d 751 (5th Cir. 1974) (citation of lower court decision).
  \item \textsuperscript{126} \textit{Burrows}, 529 P.2d at 590.
\end{itemize}
The seminal right-to-privacy case in financial matters is a relatively old English case, *Tournier v. National Provincial and Union Bank of England*.\(^{127}\) The plaintiff in this case was overdrawn at his bank by nine pounds, eight shillings. He promised to pay off the overdraft in increments of one pound a week, but, after three weeks, failed to make good on his promise. Subsequently, the bank noted that Tournier had received a check made out to him in the amount of forty-five pounds and that he had endorsed the check over to a Mr. Lloyd. The bank became aware of the check because it was drawn on the account of one of the bank's other customers. When the bank noticed that Tournier had endorsed the check over to Mr. Lloyd instead of using it to pay off his overdraft, the bank called Mr. Lloyd's bank and was told that he was a "bookmaker."\(^{128}\) The bank then called Tournier's employer to find a current address for Tournier. In response to questions from the employer, the bank disclosed the fact that Tournier was overdrawn at the bank and stated that: "As we have been able to trace a cheque or cheques to a bookmaker we are afraid he is mixed up with bookmakers."\(^{129}\) Shortly thereafter, Tournier's employment contract was not renewed, although it is unclear whether this event was due to the bank's unfavorable disclosure or, as the jury found, the fact that the company's business "was not brisk."\(^{130}\)

Each of the three judges hearing the case on appeal ruled, in separate decisions, that there was, "as a matter of law," no "absolute contract" of confidentiality.\(^{131}\) Instead, they held that "it was an implied term of the contract between the plaintiff and the bank that they would not disclose to anyone any of the plaintiff's business with the bank or matters arising therefrom, or the nature or state of his account, or any transactions relating thereto."\(^{132}\)


\(^{128}\) *Tournier*, 1 K.B. at 461.

\(^{129}\) Id.

\(^{130}\) Id.

\(^{131}\) Id. This holding was in spite of the fact that the bank had written on Tournier's passbook, as well as on those of all its customers: "The officers of the Bank are bound to secrecy as regards the transactions of its customers." Id.

\(^{132}\) Id. Curiously, though, one judge suggested that the disclosure that Tournier had endorsed over a check to a bookmaker might not be protected since that piece of information did not result from any activity in Tournier's account, but rather in another customer's account. Id.
The contract, though, according to the court, was a qualified one that had the following exceptions:

(1) Where the disclosure is under compulsion by law.
(2) Where there is a duty to the public to disclose.
(3) Where the interests of the bank require disclosure.
(4) Where the disclosure is made by the express or implied consent of the customer.  

This four-part test controlled many subsequent court cases. In Peterson, however, the court used a different formula. The facts of this case were actually quite similar to Tournier. In Peterson, the managing officer of a company had approached the bank and had asked the bank to tell him if any of the company's employees "might be doing anything that might bring discredit to the company." Subsequently, an officer of the bank wrote a letter to the company's managing officer saying: "the personal finances of your local representative have deteriorated to the point where much unfavorable criticism is being voiced. We have returned a large number of checks for not sufficient funds, and I fear that some of the holders of these checks could take legal action." The officer later showed the managing officer the plaintiff's actual accounts.

In reviewing the facts of the case, the court applied the following four-part test for privacy, without even referring to Tournier:

(1) Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
(2) Public disclosure of embarrassing private facts about the plaintiff.

133. Id.
135. Id. at 287; see infra note 139 and accompanying text.
136. Id. at 286.
137. Id.
138. Id.
Publicity which places the plaintiff in a false light in the public eye.

Appropriation, for the defendant’s advantage, of the plaintiff’s name or likeness.  

In spite of the apparent applicability of the first two tests, the court held—with very little discussion—that there was no violation or breach of privacy because the bank account information was not disclosed to the public—just to the employer.  

This, the court held, was not enough to satisfy the requirements of the privacy tests.  

Although the court refused to find an invasion of privacy, it held that there was an agency relationship between the bank and the customer and that, according to the Restatement of Law of Agency, the bank had “a duty to the [customer] not to use or communicate information confidentially given him by the [customer].”  

Accordingly, the court found that there was an implied contract between the bank and the customer that the bank breached:

It is implicit in the contract of the bank with its customer or depositor that no information may be disclosed by the bank or its employees concerning the customer’s or depositor’s account, and that, unless authorized by law or by the customer or depositor, the bank must be held liable for breach of the implied contract.  

What is fascinating here is that although the court specifically and emphatically rejected the violation of privacy claim and, instead, relied on an agency theory, coupled with an implied contract theory, the court also referenced as applicable the people’s Fourth

---

139. Id. at 287. Instead of setting forth a list of exceptions to the general rule of privacy, the Peterson court tried to articulate an actual rule for privacy.

140. Peterson, 367 P.2d at 288.

141. Id. The decision, though, failed to discuss the possible applicability of the first test, which, as the court spelled out, did not “depend upon publicity.” Id. at 287.

142. Id. at 289-90; see also, Dr. John Breslin, Privacy - the Civil Liberties Issue, 14 DICK. J. INT’L. L. 455, 459-60 (1996).

143. Peterson, 367 P.2d at 290.
Amendment right to be secure in their papers, as well as a state statute that protected "the sanctity of the privacy of bank accounts." However, the court completely neglected to discuss or analyze the applicability of either the Fourth Amendment or the state statute to the case.

In the case of Suburban Trust Co. v. Waller, the facts were very straight-forward, yet produced a complicated result. In this case, Mr. Waller deposited $800 in cash into an account that he had opened only the previous month. His companion deposited an identical amount in an account he had just opened that same day. The cash they deposited consisted of sequentially numbered fifty and one hundred dollar bills. The tellers handling the transaction brought the deposits to the attention of the bank's security officer. He, in turn, contacted the local law enforcement authorities and learned that there had been a recent robbery in the area in which $3,000 in fifty and one hundred dollar bills had been taken. In addition, the description that the authorities gave of the suspects generally matched the description of the bank's two customers. When the security officer was told this information, he became even more suspicious of the two customers and, understandably and properly, disclosed their identity to the authorities. The victim later identified Waller as one of the suspects and, on that basis, he was arrested.

As it turned out, Waller apparently did not commit the crime. He had received a tax refund check for an undisclosed amount, and when he went to cash it at the bank, he was rebuffed because he did not have enough collected funds in his

144. *Id.* at 289.
145. *Id.* at 290.
147. *Id.* at 760.
148. *Id.*
149. *Id.*
150. *Id.* at 760-61.
151. *Id.* at 761.
152. *Suburban Trust Co., 408 A.2d at 761.*
153. *Id.*
154. *Id.*
155. *Id.*
156. *Id.* at 760.
account to cover the check.\textsuperscript{157} He then physically took the check to the Treasury Department where he got the check cashed, apparently with newly minted money, and returned to the bank to deposit at least some of that money.\textsuperscript{158}

After the charges were dismissed, Waller sued the bank for invasion of privacy and breach of an implied contract.\textsuperscript{159} The trial court issued a direct verdict against Waller on the invasion of privacy claim, but issued a directed verdict in his favor on the issue of the bank’s liability on the breach of implied contract count.\textsuperscript{160} The judge allowed only the issue of damages to go to the jury, which awarded Waller $50,000 in compensatory damages.\textsuperscript{161} The bank appealed the verdict on three grounds:

(1) The bank’s limited disclosure of account related information to the police was reasonable.
(2) The bank’s actions were not the proximate cause of Waller’s damages.
(3) There was inadequate evidence as to Waller’s alleged loss of reputation.\textsuperscript{162}

The appellate court, in ruling on the case, relied on \textit{Tournier} to hold: “Courts have recognized the special considerations inherent in the bank-depositor relationship and have not hesitated to find that a bank implicitly warrants to maintain, in strict confidence, information regarding its depositor’s affairs.”\textsuperscript{163}

The court also quoted \textit{Peterson} with favor, but failed to do so in a way that indicated that there was a balancing of any kind to perform.\textsuperscript{164} Instead, the court quoted only the following section from \textit{Peterson}:

\begin{itemize}
\item \textsuperscript{157} \textit{Id.} Why any bank would require a customer to “cover” a Government issued tax refund check is unclear, unless the bank thought that the check was stolen or fraudulent.
\item \textsuperscript{158} \textit{Suburban Trust Co.}, 408 A.2d at 760.
\item \textsuperscript{159} \textit{Id.} at 761.
\item \textsuperscript{160} \textit{Id.}
\item \textsuperscript{161} \textit{Id.} at 760-61.
\item \textsuperscript{162} \textit{Id.} at 761.
\item \textsuperscript{163} \textit{Id.} at 762.
\item \textsuperscript{164} \textit{Suburban Trust Co.}, 408 A.2d. at 763.
\end{itemize}
It is inconceivable that a bank would at any time consider itself at liberty to disclose the intimate details of its depositors' accounts. Inviolable secrecy is one of the inherent and fundamental precepts of the relationship of the bank and its customers or depositors. . . .

It is implicit in the contract of the bank with its customer or depositor that no information may be disclosed by the bank or its employees concerning the customer’s or depositor’s account. . . .165

In fact, the Peterson court held that the contract between the banker and the customer was contingent on the bank’s “duty of disclosure.”166 This is the same duty that the court in Indiana National Bank v. Chapman,167 ruled did require a disclosure to law enforcement authorities.168

Reflecting its rigidity, the Suburban court rejected the four part test of Tournier on the grounds that it conferred “upon a bank entirely too much discretion.”169 The court’s decision, though, seems to have swung completely the other way. To bolster its holding, the court quoted with favor a state law, which was not yet in effect at the time of the events of this case, for the proposition that “banks may not, absent legal compulsion or express or implied authorization from the depositor concerned, reveal any information to any one, including police and other government agencies, about the depositor’s dealings with the bank.”170

Unfortunately, the overly glib court171 refused to even consider the reasonableness of the bank’s action and upheld the lower court’s determination of the bank’s liability on a directed verdict without any discussion of the proximate cause issue. In this

165. Id. (citing Peterson v. Idaho First Nat’l Bank, 367 P.2d 284, 290 (1961)).
168. Id. at 482; see also Tew v. Chase Manhattan Bank, N.A., 728 F. Supp. 1551,1566 (S.D. Fla. 1990).
170. Id. at 765. See Breslin, supra note 142, at 462.
171. Throughout the decision, the court made unnecessary sarcastic remarks and used colloquialisms that it took pains to explain in footnotes. See generally Suburban Trust Co., 408 A.2d 758 (Md. Ct. Spec. App. 1979).
regard, it is hard to accept the notion that, as a matter of law, a bank can be held responsible for an arrest that was a governmental decision and action based on the positive identification by the victim. Subsequent courts have disagreed with the Suburban decision in general and on this point of proximate cause specifically, as discussed later.

The holding in Suburban, of course, does not represent the state of the law today. Pursuant to various regulations, a bank must report suspicious activity, which is clearly all that the bank in this case did. Furthermore, a bank is now protected by a "safe harbor," as discussed below.

One of the cases to disagree with the Suburban decision was Indiana National Bank v. Chapman. In that case, the State Police were investigating Chapman for possible arson and insurance fraud stemming from the discovery of his car, abandoned and burned out. The officer in charge of the investigation, Sergeant York, contacted the bank where Chapman had his car loan and was told that the car had been slated for repossession at one time, due to late payments. As it turned out, however, there was a dispute over the payments, and, apparently, Chapman had only been minimally late with his payments, if ever.

Chapman was charged with arson, but when the evidence against him did not pan out, the prosecutor moved for the charges

172. Id. Ironically, the court actually relented on the bank's third claim to the effect that there was, in the words of the court, "no evidence that Waller's reputation was damaged." Id. at 766. Since the District Court had ruled out the possibility of punitive damages and that holding had not been appealed, it would seem that the case should have been dismissed in favor of the bank. However, the court sent the case back down to be tried all over again. Id.


175. 31 U.S.C. § 5318(g)(3) (1994). While the reporting requirements entail a dollar threshold for non-insiders, the safe harbor protects the banks for even voluntary reporting.


177. Id. at 476.

178. Id.

179. Id. at 476-77.
to be dismissed. Subsequently, Chapman sued the bank and was awarded almost $90,000.

In reviewing the case on appeal, the court held that the bank was entitled to respond to a legitimate law enforcement inquiry and, as such, had a qualified privilege to the normal rule that a banker should not divulge bank-related information without the consent of the customer:

"[w]e hold a bank impliedly contracts only that it will not reveal a customer's financial status unless a public duty arises. Communication to legitimate law enforcement inquiry meets the public duty test."

The court also relied on relevant state law to support its reasoning: "[t]he Indiana law of privacy recognizes an invasion only if the matter is not of public concern, and case law in our state indicates that a person does not legitimately expect his affairs with third parties to be kept private from law enforcement officers conducting an investigation."

In another case, Velasquez-Campuzano v. Marfa National Bank, the plaintiffs went to the bank in order to redeem two certificates of deposit and to make a large cash withdrawal so they could transport the funds to Mexico and take advantage of higher interest rates that existed in that country at that time. However, when they were informed that a Currency Transaction Report (CTR) would have to be filed, they revised their requests so that they left the bank with less than $10,000 in cash. The bank suspected the couple of attempting to engage in structuring, in violation of 31 U.S.C. § 5324, and, accordingly, filed a Criminal Referral Form. Even though the husband later pled guilty to structuring, making false statements, and causing the bank to fail

180. Id. at 447.
181. Id. at 476.
182. Ind. Nat'l Bank, 482 N.E.2d. at 478, 480-82.
183. Id. at 482. In reaching this holding, the court specifically rejected the Suburban Trust rule and implicitly adopted the second privacy exemption set forth in the Tournier case: "where there is a duty to the public to disclose." Tournier v. Nat'l Provincial and Union Bank of England, 1 K.B. 461 (1923).
184. Id.
186. Id. at 1418.
187. Id.
188. Id. at 1418-19.
189. Id.
to file a CTR, the couple nonetheless brought suit against the bank for violations of the RFPA, state law, their Fourth Amendment rights to privacy, and an implied "condition of confidentiality."\textsuperscript{190}

In granting the bank’s motion for summary judgment,\textsuperscript{191} the court held first that the RFPA did not apply because the bank’s disclosures were compelled by federal law.\textsuperscript{192} Second, in denying the other claims, the court noted that "the Supreme Court in Miller has declined to recognize a constitutional right to privacy in banking records."\textsuperscript{193}

In passing, the court also noted that Congress had amended the BSA by providing for a safe harbor to protect banks in situations like the one raised in this case "by explicitly providing blanket immunity from civil liability for a bank’s disclosure of information required by Federal law."\textsuperscript{194} Although this safe harbor, due to its lack of retroactivity, was not applicable to \textit{Marfa},\textsuperscript{195} the safe harbor became an important part of a subsequent case, \textit{Merrill, Lynch v. Green}.\textsuperscript{196}

In this case, Merrill Lynch had received a tip of suspicious activity about one of its clients from the British Customs.\textsuperscript{197} Merrill Lynch apparently reported the suspicions to the U.S. authorities, and, eventually, $1.6 million was seized from the customer’s account as "proceeds from money laundering and illegal drug-trafficking."\textsuperscript{198} The customer then brought an arbitration claim against Merrill Lynch for "colluding" with the government and for mishandling his account.\textsuperscript{199} In upholding Merrill Lynch’s request for a preliminary injunction against the customer from proceeding with the arbitration claim, the court held that Merrill Lynch had acted appropriately and, further, was

\textsuperscript{190} Id.
\textsuperscript{192} Id. at 1420.
\textsuperscript{193} Id. at 1424.
\textsuperscript{194} Id. at 1423. The safe harbor was codified at 31 U.S.C. § 5318(g)(3).
\textsuperscript{195} Id. at 1424.
\textsuperscript{197} Id. at 943.
\textsuperscript{198} Id.
\textsuperscript{199} Id.
immune under the safe harbor of the BSA found at 31 U.S.C. § 5318.\textsuperscript{200}

In a subsequent case, \textit{Lopez v. First Union National Bank},\textsuperscript{201} the holding at the district court level was similarly that, as a result of the safe harbor, the bank had "blanket immunity from civil liability under any federal or state law when reporting suspicious transactions."\textsuperscript{202} In a comparable case, \textit{Coronado v. BankAtlantic Bancorp},\textsuperscript{203} the district court, located in the same judicial district as the court in \textit{Lopez}, quoted the \textit{Lopez} decision and delivered the same ruling.\textsuperscript{204}

On appeal, however, the Eleventh Circuit joined \textit{Lopez} and \textit{Coronado} and overturned both of them.\textsuperscript{205} In reviewing these cases, the appellate court noted that they were each brought on the basis of a motion to dismiss the case for failure to state a claim.\textsuperscript{206} Consequently, the court was required to accept the plaintiffs' complaints as true.\textsuperscript{207}

In \textit{Lopez}, the plaintiffs alleged that the bank had provided law enforcement authorities with access to their bank records "based solely on the 'verbal instructions' of federal law enforcement authorities."\textsuperscript{208} In \textit{Coronado}, the complaint alleged that the bank had improperly disclosed protected bank account information from 1,100 different accounts.\textsuperscript{209}

In reviewing the facts of each case, the appellate court held that the safe harbor granted banks immunity from liability for three different types of disclosure:

1. A disclosure of any possible violation of law or regulation.
2. A disclosure pursuant to § 5318(g).
3. A disclosure pursuant to any other authority.\textsuperscript{210}

\textsuperscript{200} \textit{Id.} at 943-44.
\textsuperscript{202} \textit{Id.} at 864-65.
\textsuperscript{204} \textit{Id.} at 1026.
\textsuperscript{205} \textit{Lopez v. First Union Nat'l Bank of Fla.}, 129 F.3d 1186, 1188 (11th Cir. 1997).
\textsuperscript{206} \textit{Id.} at 1188-89, 1194.
\textsuperscript{207} \textit{Id.}
\textsuperscript{208} \textit{Id.} at 1188.
\textsuperscript{209} \textit{Id.} at 1194-95.
\textsuperscript{210} \textit{Id.} at 1191.
After considerable discussion of these provisions, the court held that, in order to avail themselves of any of the provisions, the banks also had to show that they had acted in good faith.\textsuperscript{211} The court also specifically held that the alleged oral request from a law enforcement authority in *Lopez* was insufficient to satisfy the good faith requirement.\textsuperscript{212} Similarly, in *Coronado*, even though the complaint had alleged that the bank had noted suspicious activity, unusual amounts of money, and unusual movements of money, that did not, on its own, justify the bank’s disclosure of information from 1,100 different accounts.\textsuperscript{213} Consequently, the banks were faced with the unfortunate result that if the plaintiffs’ complaints filed against them did not allege that the banks were acting in good faith—a fact that no complaint would ever be expected to allege—the banks could not have the courts dismiss the cases.\textsuperscript{214} Pursuant to the court’s ruling, the banks would almost always have to litigate any actions brought against them in these circumstances, regardless of how inaccurate the complaints might be.

In *Coronado*, the complaint, in fact, turned out to be wholly inaccurate.\textsuperscript{215} On the second appeal, the Eleventh Circuit was persuaded by the bank’s motion for summary judgment that the bank had received a legitimate grand jury subpoena for bank records covering almost 1,100 accounts.\textsuperscript{216} Apparently, BankAtlantic had acquired another bank, Megabank, as well as the latter’s international division that contained approximately 1,100 accounts.\textsuperscript{217} After several audits, BankAtlantic determined that there were suspicious pouches coming from Bogota, Columbia into the bank’s newly acquired international division and that there were millions of dollars flowing into and out of Columbia-

\textsuperscript{211} *Lopez*, 129 F.3d at 1192-93, 1195-96.

\textsuperscript{212} *Id.* at 1193.

\textsuperscript{213} *Id.* at 1195.

\textsuperscript{214} *Id.* at 1193, 1195-96.

\textsuperscript{215} Coronado v. BankAtlantic Bancorp, 222 F.3d 1315, 1322 (11th Cir. 2000).

\textsuperscript{216} *Id.* at 1316-17, 1319, 1321. This determination was made only after two district court decisions, “several motions for discovery” and two court of appeals decisions. *Id.* This saga took over three and a half years, from before January 22, 1997, when the first district court decision was handed down, 951 F. Supp. 1025 (S.D. Fla. 1997), to August 18, 2000, when the second Eleventh Circuit decision was handed down, 222 F.3d 1315 (11th Cir. 2000).

\textsuperscript{217} *Coronado*, 222 F.3d at 1317.
based accounts each month. Accordingly, the bank alerted the authorities, but provided them specific information about only five of the most obviously suspicious accounts. After some investigation, law enforcement authorities responded with the grand jury subpoena referenced above.

Based on this record, the Eleventh Circuit held that the lower court's granting of the bank's motion for summary judgment was proper. What is fascinating about the court's decision is not the holding, but rather the fact that nowhere in the decision is the term "good faith" mentioned. In fact, the court's references to the safe harbor are in very strong, albeit ironic, terms: "because disclosure of financial information—either spontaneously or after a request from the government—could possibly lead to litigation with disgruntled customers like Coronado, the Annunzio-Wylie Act granted immunity to banks making disclosures."

In another appellate decision on the issue, Lee v. Bankers Trust Co., the Second Circuit specifically rejected any notion that there had to be a showing of good faith in order for a bank to take advantage of the BSA safe harbor provision. As set forth by the court:

The safe harbor provision applies, regardless of whether the SAR [Suspicious Activity Report] is filed as required by the Act or in an excess of caution.

The plain language of the safe harbor provision describes an unqualified privilege, never mentioning good faith or any suggestive analogue thereof. The Act broadly and unambiguously provides for immunity from any law (except the federal Constitution) for any statement made in [a] SAR by anyone connected to a financial institution. There is

218. Id.
219. Id.
220. Id.
221. Id. at 1322.
222. Id. at 1319.
224. Id. at 544-45.
not even a hint that the statements must be made in good faith in order to benefit from immunity. Based on the unambiguous language of the Act, Bankers Trust enjoys immunity from liability for its filing of, or any statement made in, a SAR.225

In addition to the difficulty of having to litigate a frivolous case against a disgruntled customer, as set forth in the last Eleventh Circuit’s decision in Coronado,226 the Second Circuit in Lee pointed out the following problem:

Under Plaintiff’s theory, he can allege, on information and belief, that a bank filed a SAR containing allegedly defamatory statements that were not made in good faith. If the bank sought summary judgment, it would then have to establish that the statements in the SAR were made in good faith, but it would be prohibited by law both from disclosing the filing or the contents of a SAR. It flies in the face of common sense to assert that Congress sought to impale financial institutions on the horns of such a dilemma.227

In the last case on this issue, Stoutt v. Banco Popular de Puerto Rico,228 the court agreed with the Lee decision.229 In Stoutt, a customer of the bank, who was a resident of the British Virgin

---

225. Id. at 544. In addition to referencing the “plain language” of the statute, the court bolstered its holding by referencing the legislative history as well:

Finally, although the safe harbor provision is unambiguous, and does not require resort to legislative history, the history of the Act demonstrates that Congress did not intend to limit protection to statements made in good faith. An earlier draft of the safe harbor provision included an explicit good faith requirement for statements made in a SAR. However, the requirement was dropped.

Id.

226. Coronado, 222 F.3d at 1319.
227. Lee, 166 F.3d at 544.
229. Id. at 174-75.
Islands, wanted to borrow $1.5 million from the bank. In order to secure the loan, the customer had a plan whereby he would lease $10 million in United States Treasury bills, paying a monthly interest of $300,000. The catch was that he had to pay an "advance fee" of $300,000. In order to do so, he had to overdraft his account at the bank. It took the customer over a month to realize that the scheme of leasing the Treasury bills was a scam. By that time, the bank had become suspicious of the customer's actions and excuses and, consequently, filed a SAR. The customer was arrested, but the case was later dropped due to insufficient evidence. At that point, the customer filed suit against the bank "alleging unlawful arrest, malicious prosecution and illegal incarceration."

The court, in ruling in favor of the bank's motion for summary judgment, held that the "safe harbor" provision read literally grants absolute immunity from any federal and or state cause of action for disclosure of possible violations of law by a financial institution to the appropriate federal law enforcement agency. The court specifically found the initial appellate decision in Lopez to be "unpersuasive" and, instead, agreed with Lee for the reasons set forth in that decision.

In specifically rejecting the customer's claims, the court noted that the bank:

... did not effectuate the arrest and a grand jury did find probable cause.

Notwithstanding, Plaintiff urges this court to require financial institutions to make a finding of probable cause prior to the filing [of] a SAR. However,

230. Id. at 169.
231. Id.
232. Id.
233. Id. at 169-70.
235. Id.
236. Id. at 171.
237. Id. at 168.
238. Id. at 173.
239. Id. at 175.
240. Stoutt, 158 F.Supp. 2d at 174-75.
requiring financial institutions to reach a finding of probable cause before filing a SAR would subject them to a drawn out discovery process similar to the imposition of a good faith requirement.\textsuperscript{241}

This is exactly what happened, of course, in \textit{Coronado}.\textsuperscript{242} It also underscores yet one more reason why the safe harbor provision should be construed broadly, as the initial district court decision in \textit{Lopez} indicated:

\begin{quote}
[I]n the Congressional Record of January 5, 1993, there is an Extension of Remarks from the House of Representatives regarding the Annunzio-Wylie Anti-Money Laundering Act. \textit{See} 139 Cong. Rec. E57-02 (1993). A letter written by Congressman Frank Annunzio, Chairman of the Subcommittee on Financial Institutions, Washington, D.C. and author of the Act, was included as part of the Congressional Record, and notes his deep concern that financial institutions should be free to report suspicious transactions without fear of civil liability. In this letter, Congressman Annunzio states that Section 5318 of Title 31 of the U.S.C. was amended in order “to provide the broadest possible exemption from civil liability for reporting of suspicious transactions.” \textit{See} 139 Cong. Rec. E57-02 (1993). “... Congress wanted to [en]sure that financial institutions which reported suspicious transactions should not be held liable to any person under any law, Federal, state or local, for making such disclosures.” \textit{Id}.\textsuperscript{243}
\end{quote}

These cases demonstrate that, while there is an implied contract of confidentiality, it is not an absolute right of confidentiality. While the first two cases discussed above indicate the potential liability in disclosing confidential information to

\textsuperscript{241} \textit{Id.} at 175.
\textsuperscript{242} \textit{Coronado} v. BankAtlantic Bancorp, 222 F.3d 1315, 1317 (11th Cir. 2000).
employers,\textsuperscript{244} it is clear that the banks have a duty to disclose suspicious activity and potential violations of criminal law to law enforcement authorities.\textsuperscript{245} While this obligation is now a matter of statute and regulation, it is one that has existed for a long time. For instance, in \textit{Tournier}, the court held that one of the conditions to the implied contract of confidentiality is the "duty to the public to disclose."\textsuperscript{246} This has been specifically interpreted to include the duty to disclose potential violations of criminal law.\textsuperscript{247} Importantly, the BSA safe harbor now protects the bank from liability in making such disclosures to law enforcement authorities.\textsuperscript{248} The trend of the cases in construing this safe harbor appears to be strongly in favor of holding that it provides the banks absolute immunity and does not require them to establish in court their good faith.\textsuperscript{249} As set forth in these cases, the logic and legislative history are clearly in favor of this interpretation.\textsuperscript{250} The banking agencies are also in accord with the position:

\begin{quote}
[T]he OCC and other Federal financial institutions regulatory agencies believe that the [BSA] 'safe harbor' provides complete immunity to any institution that reports a potential crime by filing a Suspicious Activity Report (SAR) in accordance with the instructions on the SAR form, or by
\end{quote}


\textsuperscript{246} Tournier v. Nat'l Provincial and Union Bank of England, 1 K.B. 461 (1923). The initial cases to the contrary dealt primarily with informal requests to the bank from law enforcement authorities, as opposed to determinations by the bank that something was suspicious. Burrows v. Superior Court of San Bernardino County, 529 P.2d 590, 591(Cal. 1975); Suburban Trust Co. v. Waller, 408 A.2d 758, 760 (Md. Ct. Spec. App. 1979).


\textsuperscript{250} Lee, 166 F.3d at 544; Strott, 158 F.Supp. at 175.

\section*{VII. Constitutionality of the Bank Secrecy Act}

With regard to the cases pertaining to privacy rights and banks' liability for disseminating customers' financial information, it is important to note that, since 1970, the cases have been affected by the passage of the BSA. Most significantly, \textit{Miller}, in holding that there was no right to privacy with regard to bank records, relied heavily on the fact that the BSA required banks to maintain certain records.\footnote{United States v. Miller, 425 U.S. 435, 442-43 (1976).} While, at the time of \textit{Miller}, the Supreme Court had already upheld the constitutionality of the BSA,\footnote{California Bankers Ass'n v. Shultz, 416 U.S. 21, 77 (1974).} it is important to go back and review the constitutional attack on the BSA and the courts' analysis of the arguments.

In the primary case that challenged the constitutionality of the BSA, several bank customers, a bank, the California Bankers Association and the American Civil Liberties Association brought suit against John Connally, the then Secretary of the Treasury and the individual responsible for implementing the BSA.\footnote{Stark v. Connally, 347 F. Supp. 1242, 1243-44 (N.D. Cal. 1972).} The plaintiffs sought to enjoin the Secretary from enforcing the BSA and its implementing regulations on the grounds that enforcement of the statute and the regulations would pose "grave and irreparable injury to their constitutional rights - [including] their right to freedom from unreasonable search; [and] their constitutional right of privacy."\footnote{\textit{Id.} at 1244.} In analyzing the BSA, the court broke the statute down into three components: (1) record-keeping; (2) reporting of foreign financial transactions; and (3) reporting of domestic financial transactions.\footnote{\textit{Id.} at 1244-45.} Without any real substantive discussion, the court found that the record-keeping requirements did not create any constitutional violation.\footnote{\textit{Id.} at 1244.}

With regard to the requirements for reporting foreign transactions, such as the requirement to report the transportation
of monetary instruments in excess of $5,000 into or out of the United States, the court held that they too were not unconstitutional. In reaching this holding, the court was mindful that "the Courts should not substitute their judgment for that of the Congress." The court also noted that the "Supreme Court, when dealing with matters of reporting to and surveillance by the executive, has traditionally recognized a distinction between domestic surveillance, on the one hand, and surveillance where foreign nations are involved, pointing out that what might be impermissible in domestic cases may be constitutional where foreign powers are involved."

The court, however, found that the domestic reporting requirements were unconstitutional. First, the court phrased the question on this issue in a way that dictated the result:

The question is whether these provisions, broadly authorizing an executive agency of the government to require financial institutions and parties to or participants in transactions with them, to routinely report to it, without previous judicial or administrative summons, subpoena or warrant, the detail of almost every conceivable financial transaction as a surveillance device for the discovery of possible wrongdoing on the part of bank customers, is such an invasion of a citizen's right of privacy as amounts to an unreasonable search within the meaning of the Fourth Amendment.

Then, the court provided the answer to the issue by virtually repeating the question:

[T]he Act in question, insofar as it authorizes the Secretary to require virtually unlimited reporting from banks and their customers of domestic financial transactions as a surveillance device for the

258. Id. at 1244-45.
260. Id.
261. Id. at 1251.
262. Id. at 1246.
alleged purpose of discovering possible, but unspecified, wrongdoing among the citizenry, so far transcends the constitutional limits, as laid down by the United States Supreme Court for this kind of legislation, as to unreasonably invade the right of privacy protected by The Bill of Rights, particularly the Fourth Amendment provision protecting "the right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures." 263

Unfortunately, the court failed to engage in any kind of balancing effort between people's privacy rights and the need for certain domestic reports. More importantly, the court failed to take into consideration that the reporting requirements authorized by the BSA were not self-implementing. The court actually acknowledged that "to date the Secretary has required reporting only by the financial institutions and then only of currency transactions over $10,000." 264 However, the court did not base its analysis of the reasonableness of the statutory and regulatory scheme on what was before it. Rather, the court improperly chose to use extreme language to project what might be required ("the Act... authorizes the Secretary to require virtually unlimited reporting... as a surveillance device." 265) without analyzing what was really required.

The Supreme Court, in its decision reversing the district court, 266 specifically rejected the lower court's framing of the question quoted immediately above:

Since, as we have observed earlier in this opinion, the statute is not self-executing, and were the Secretary to take no action whatever under his authority there would be no possibility of criminal or civil sanctions being imposed on anyone, the District Court was wrong in framing the question in

263. Id. at 1251.
264. Id. at 1246.
266. California Bankers Ass'n. v. Shultz, 416 U.S. 21 (1974). This case was appealed directly from the District Court to the Supreme Court.
this manner. The question is not what sort of reporting requirements might have been imposed by the Secretary under the broad authority given him in the Act, but rather what sort of reporting requirements he did in fact impose under that authority. 267

In upholding the constitutionality of the BSA, the Court favorably noted the important reason for the legislation: “The express purpose of the Act is to require the maintenance of records, and the making of certain reports, which ‘have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings.’” 268

The Court went on to note that the reporting requirements established by the Secretary pursuant to the BSA were not new or unusual:

[M]ost of the recordkeeping requirements imposed by the Secretary under the Act merely require the banks to keep records which most of them had in the past voluntarily kept and retained, and . . . much of the required reporting of domestic transactions had been required by earlier Treasury regulations in effect for nearly 30 years. 269

Prior to the enactment of the Act, financial institutions had been providing reports of their customers’ large currency transactions pursuant to regulations promulgated by the Secretary of Treasury which had required reports of all currency transactions that, in the judgment of the institution, exceeded those “commensurate with the customary conduct of the business, industry or profession of the person or organization concerned.” 270

267. Id. at 64 (emphasis in the original); see id. at 78 (Powell, J., concurring).
268. Id. at 26.
269. Id. at 29-30.
270. Id. at 37 (citations omitted). The Court cited to a regulation passed in 1949 that required the reporting of transactions involving $1,000 or more in denominations of $50 or more, or $10,000 or more in any denominations. Id.
The preexistence of these reporting requirements was also noted by Congress in passing the BSA:

Criminals deal in money—cash or its equivalent. The deposit and withdrawal of large amounts of currency or its equivalent (monetary instruments) under unusual circumstances may betray a criminal activity. . . . Reports along this line have been required by Treasury Department regulations for a number of years (31 CFR 102). 271

In fact, the Senate Report on the legislation explained that the BSA would provide the specificity and clarity that the previous legislation and regulations lacked: "under existing Treasury regulations, currency reports are required on transactions involving any amount which is unusual in the judgment of the financial institution. It is anticipated that the regulations under the proposed legislation will define more objectively what constitutes an "unusual" currency transaction." 272

In further addressing the alleged burden that the BSA reporting requirements might create, the Court reiterated the straightforward nature of the requirements:

We proceed then to consider the initial contention of the bank plaintiffs that the recordkeeping requirements imposed by the Secretary's regulations under the authority of Title I deprive the banks of due process by imposing unreasonable burdens upon them, and by seeking to make the banks the agents of the government in surveillance of its citizens. Such recordkeeping requirements are scarcely a novelty. 273

273. California Bankers Ass'n v. Shultz, 416 U.S. 21, 45 (1974). The Court went on to list a number of the existing reporting requirements. Id. at 45-46, n.19.
Pursuing the burden issue further, the Court noted that the cost burdens on the banks were not unreasonable, and could be justified by the fact that the banks were not "complete bystanders" or "conscripted neutrals in transactions involving negotiable instruments, but parties to the instruments with a substantial stake in their continued availability and acceptance." Moreover, the Court stated that, at least with regard to banks whose deposits were insured by the federal government, the reporting requirement imposed could be viewed simply as a "condition" to doing business.

In addition, the Court thought that it was important to focus on the fact that the Secretary was only requiring reports of currency of more than $10,000. Consequently, the Court had "no difficulty ... in determining that the Secretary's requirements for the reporting of domestic financial transactions abridge no Fourth Amendment right of the banks themselves." As set forth by the Court: "the regulations do not impose unreasonable reporting requirements on the banks. The regulations require the reporting of information with respect to abnormally large transactions in currency, much of which information the bank as a party to the transaction already possesses or would acquire in its own interest."

In contrast to the well-reasoned and straightforward majority opinion, the dissent used emotion and hyperbole to argue its position:

This [Act] will cost the banks, it is estimated, over $6 million a year.... Moreover, they must spy on their customers. The Bank Secrecy Act requires

274. Id. at 50.
275. Id. at 48.
276. Id. at 48-49; see id. at 52 ("all of the records which the Secretary requires to be kept pertain to transactions to which the bank was itself a party"); id. at 66 ("The bank is not a mere stranger or bystander with respect to the transactions which it is required to record or report. The bank is itself a party to each of these transactions, earns portions of its income from conducting such transactions, and in the past may have kept records of similar transactions on a voluntary basis for its own purposes.").
277. Id. at 50.
278. Id. at 39, 63.
279. California Bankers Ass'n, 416 U.S. at 66.
280. Id. at 67.
banks to record and retain the details of their customers' financial lives.\textsuperscript{281}

It would be highly useful to governmental espionage to have like reports from all our bookstores, all our hardware and retail stores, all our drugstores. These records too might be "useful" in criminal investigations.

One's reading habits furnish telltale clues to those who are bent on bending us to one point of view. What one buys at the hardware and retail stores may furnish clues to potential uses of wires, soap powders, and the like used by criminals. A mandatory recording of all telephone conversations would be better than the recording of checks under the Bank Secrecy Act, if Big Brother is to have his way.\ldots

It is, I submit, sheer nonsense to agree with the Secretary that all bank records of every citizen "have a high degree of usefulness in criminal, tax, or regulatory investigations of proceedings." That is unadulterated nonsense unless we are to assume that every citizen is a crook, an assumption I cannot make.

Since the banking transactions of an individual give a fairly accurate account of his religion, ideology, opinions, and interests, a regulation impounding them and making them automatically available to all federal investigative agencies is a sledgehammer approach to a problem that only a delicate scalpel can manage.\textsuperscript{282}

While this is colorful and exciting rhetoric, it is wide of the mark. First, as the majority indicated, as well as Justice Powell in his concurring opinion, the review of the constitutionality of the Act

\textsuperscript{281} \textit{Id.} at 80.

\textsuperscript{282} \textit{Id.} at 85.
cannot be based on the extreme speculation of what the statute might authorize, but rather on what is actually before the Court. Further, the BSA does not require the banks to "spy" on their customers, but instead to simply retain copies of documents that the banks already possess, to which banks are a party, and that were found to "have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings" and to report "abnormally large transactions in currency." These reportable cash transactions in excess of $10,000 are, in fact, unusual for most individuals and certainly do not constitute "all bank records of every citizen." Nor do these large cash transactions indicate in any way a customer's "religion, ideology, opinions, and interests."

The dissent, written by Justice Douglas, complained of the government's purported use of a "sledge-hammer" instead of a "delicate scalpel." It would seem, though, that a requirement for pre-existing records to be maintained and for certain "abnormally large transactions in currency" not to be outlawed, but simply reported, is hardly heavy-handed. Rather, it appears to be the specific and measured approach Justice Douglas called for.

In United States v. Kaatz, decided a number of years after Schultz, a lower court reiterated the constitutionality of the BSA and upheld the propriety of a bank filing a "currency transaction report (CTR)." In this case, three brothers owned and ran a hardware store. An investigation into their affairs was triggered by a bank's filing of a CTR. It appears that the brothers had used $96,000 in cash to purchase a $100,000 certificate of

283. Id. at 64; see id. at 78 (Powell, J., concurring). "The question is not what sort of reporting requirements might have been imposed by the Secretary under the broad authority given him in the Act, but rather what sort of reporting requirements he did in fact impose under that authority." Id. at 64.

284. Id. at 26, 31. See 31 C.F.R. § 103.15 (2001) ("The Secretary hereby determines that the reports required by this subpart have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings.").


286. Id. at 65.

287. Id.

288. Id.

289. Id. at 67.

290. United States v. Kaatz, 705 F.2d 1237 (10th Cir. 1983).

291. Id. at 1242.

292. Id. at 1240.
At the trial, tellers from the bank testified that, almost daily, one of the brothers would present two sets of checks at the bank; one set of checks would be deposited into the hardware company's account, but the other set of checks would be cashed in aggregate amounts varying from $400 to $2,500. An IRS agent also testified at the trial that there wasn't a single instance of the company's records showing a cash payment for an over-the-counter sale. Not surprisingly, the brothers were convicted for filing false income tax returns and for evasion of income tax.

On appeal, the reviewing court upheld the convictions and held that the bank's actions were proper. Specifically, the court noted that reporting requirements of the BSA had been upheld in California Bankers Association and that, pursuant to United States v. Miller, the plaintiffs did not have a legitimate "expectation of privacy" concerning information contained in bank records.

While Miller held that individuals do not have any "legitimate 'expectation of privacy'" in their financial records maintained by banks, the records required by the BSA are not that extensive or invasive and the protections of the RFPA, passed in response to Miller, serve as an adequate protection against indiscriminate and improper dissemination of a person's financial records.

VIII. BSA Requirements

As set forth above, the BSA was passed in 1970. Since then, the BSA has been amended several times: the

293. Id.
294. Id.
295. Id.
296. Kaatz, 705 F.2d at 1239-42.
299. Kaatz, 705 F.2d at 1242. The court did not discuss the restrictions of the RFPA, which, in any event, appear to have not been relevant to the case.
300. Miller, 425 U.S. at 442.
303. See Baldwin, supra note 28, at 425.

Some of the primary provisions of the BSA are as follows:


This provision authorizes the Secretary of the Treasury to require financial institutions to make a report of certain transactions “for the payment, receipt, or transfer of United States coins or currency.” This provision was implemented primarily in 31 C.F.R. § 103.22 which requires financial institutions to file reports (Currency Transaction Reports or CTRs) “of each deposit, withdrawal, exchange of currency or other payment or transfer, by, through, or to such financial institution which involves a transaction in currency of more than $10,000.”

When a domestic financial institution is involved in a transaction for the payment, receipt, or transfer of United States coins or currency (or other monetary instruments the Secretary of the Treasury prescribes), in an amount, denomination, or amount and denomination, or under circumstances the Secretary prescribes by regulation, the institution and any other participant in the transaction the Secretary may prescribe shall file a report on the transaction at the time and in the way the Secretary prescribes....
Contrary to the concerns voiced in various cases reviewed above, to the effect that reports like this "give a fairly accurate account of [an individual's] religion, ideology, opinions, and interests . . . ," these reports of "abnormally large transactions in currency . . . " would reveal very little about the individual, except for the possibility of their being involved in illegal activity. As the legislative history to the BSA noted: "criminals deal in money—cash or its equivalent. The deposit and withdrawal of large amounts of currency or its equivalent (monetary instruments) under unusual circumstances may betray a criminal activity."

To the extent the conduct reflects the normal, appropriate activity of a business, an extensive process exists within the BSA for exempting such businesses.  


This section primarily authorizes the Secretary of the Treasury to require reports concerning accounts maintained in foreign banks. This section is implemented in 31 C.F.R. § 103.24

(a) General. This section sets forth the rules for the reporting by financial institutions of transactions in currency. The reporting obligations themselves are stated in paragraph (b) of this section. The reporting rules relating to aggregation are stated in paragraph (c) of this section. Rules permitting banks to exempt certain transactions from the reporting obligations appear in paragraph (d) of this section.

(b) Filing obligations. (1) Financial institutions other than casinos. Each financial institution other than a casino shall file a report of each deposit, withdrawal, exchange of currency or other payment or transfer, by, through, or to such financial institution which involves a transaction in currency of more than $10,000, except as otherwise provided in this section. . .

Id.

314. Id. at 67.
316. 31 C.F.R. § 103.22(d) (2001).
317. 31 U.S.C. § 5314 (1994). The relevant portion of section 5314 states:

(a) Considering the need to avoid impeding or controlling the export or import of monetary instruments and the need to avoid burdening unreasonably a person making a transaction with a
which requires individuals to report on their annual tax forms whether they hold an account in a foreign bank.\textsuperscript{318} Clearly, this provision does not affect very many people. In addition, in light of the need, as stated in the statute, for obtaining the requested information, this section would appear not to be overly invasive.

\textit{\textsuperscript{31} U.S.C. \textsection 5316—Reports on exporting and importing monetary instruments.}

This section primarily authorizes the Secretary of the Treasury to require individuals to make a report whenever they transport $10,000 in currency or monetary instruments into or out of the country.\textsuperscript{319} This section was implemented through the

foreign financial agency, the Secretary of the Treasury shall require a resident or citizen of the United States or a person in, and doing business in, the United States, to keep records, file reports, or keep records and file reports, when the resident, citizen, or person makes a transaction or maintains a relation for any person with a foreign financial agency. The records and reports shall contain the following information in the way and to the extent the Secretary prescribes:

(1) the identity and address of participants in a transaction or relationship.

(2) the legal capacity in which a participant is acting.

(3) the identity of real parties in interest.

(4) a description of the transaction.

\textit{Id.}

\textsuperscript{318} 31 C.F.R. \textsection 103.24 (2001). The relevant portion of section 103.24 states:

Reports of foreign financial accounts.

(a) Each person subject to the jurisdiction of the United States... having a financial interest in, or signature or other authority over, a bank, securities or other financial account in a foreign country shall report such relationship to the Commissioner of the Internal Revenue...”

\textit{Id.}

\textsuperscript{319} 31 U.S.C. \textsection 5316 (1994). The relevant portion of section 5316 states:

(a) Except as provided in subsection (c) of this section, a person or an agent or bailee of the person shall file a report under subsection (b) of this section when the person, agent, or bailee knowingly

(1) transports... monetary instruments of more than $10,000 at one time

(A) from a place in the United States to or through a place outside the United States; or
issuance of 31 C.F.R. § 103.23. This provision is equally important as the provision requiring the filing of CTRs, and due to the infrequency of the need for such filings, they would represent even less of a possible incursion into one's privacy.

- 12 U.S.C. § 1829b—Retention of records by insured depository institutions.

These two sections authorize the Secretary of the Treasury to require certain reports pertaining to banking accounts and certain banking transactions. The implementing regulations include 31 C.F.R. §§ 103.33 and 103.34 which require, among other things:

320. 31 C.F.R. § 103.23 (2001). The relevant portion of section 103.23 states:

Reports of transportation of currency or monetary instruments.
(a) Each person who physically transports, mails, or ships, or causes to be physically transported, mailed, or shipped... currency or other monetary instruments in an aggregate amount exceeding $10,000 at one time transported from the United States to any place outside the United States, or into the United States from any place outside the United States, shall make a report thereof. . . .

321. 12 U.S.C. § 1829(B) (2000). The relevant portion of section 1829(B) states:

(a) Congressional findings and declaration of purpose.
(1) The Congress finds that adequate records maintained by insured depository institutions have a high degree of usefulness in criminal, tax, and regulatory investigations and proceedings. . . .
(b) Recordkeeping regulations.
(1) In general.
Where the Secretary of the Treasury... determines that the maintenance of appropriate types of records and other evidence by insured depositors institutions has a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, he shall prescribe regulations to carry out the purposes of this section. . . .
(a) A record of each extension of credit in an amount in excess of $10,000;
(b) Certain information with respect to a wire transfer in the amount of $3,000 or more; and
(c) The bank to make a reasonable effort to secure and maintain a record of the taxpayer identification number with respect to each certificate of deposit sold or redeemed or each deposit or share account opened. 322


This section requires a financial institution to verify the identity of an individual who purchases a bank check with $3,000 or more in currency. 323 This requirement is implemented through

322. 31 C.F.R. § 103.33 (2001). The relevant portion of section 103.33 states:

Records to be made and retained by financial institutions.
Each financial institution shall retain either the original or a microfilm or other copy or reproduction of each of the following:
(a) A record of each extension of credit in an amount in excess of $10,000, except an extension of credit secured by an interest in real property, which record shall contain the name and address of the person to whom the extension of credit is made, the amount thereof, the nature or purpose thereof, and the date thereof.
(b) A record of each advice, request, or instruction received or given regarding any transaction resulting... in the transfer of currency or other monetary instruments, funds, checks, investment securities, or credit, of more than $10,000 to or from any person, account, or place outside of the United States....
(e) Banks. Each agent, agency, branch, or office located within the United States of a bank is subject to the requirements of this paragraph (e) with respect to a funds transfer in the amount of $3,000 or more....

Id.

31 C.F.R. § 103.34 (2001). The relevant portion of section 103.34 states:

Additional records to be made and retained by banks.
(a)(1) With respect to each certificate of deposit sold or redeemed...or each deposit or share account opened with a bank... a bank shall [make a reasonable effort to]... secure and maintain a record of the taxpayer identification number of the customer involved....

323. 31 U.S.C. § 5325 (1994). The relevant portion of section 5325 states:
31 C.F.R. § 103.29 which requires certain specific information such as name of the purchaser, date of purchase, method of payment, and the type of payment.

31 C.F.R. §103.18—Reports of banks of suspicious transactions.

In addition to these requirements, the BSA contains a requirement that financial institutions file Suspicious Activity Reports similar to those mandated by the banking agencies.324

Identification required to purchase certain monetary instruments.
(a) In general. No financial institution may issue or sell a bank check, cashier's check, traveler's check, or money order to any individual in connection with a transaction or group of such contemporaneous transactions which involves United States coins or currency . . . of $3,000 or more unless -
(1) the individual has a transaction account with such financial institution and the financial institution -
(A) verifies that fact through a signature card or other information . . . and
(B) records the method of verification . . . or
(2) the individual furnishes the financial institution with such forms of identification as the Secretary of the Treasury may require in regulations . . . .

Id.

324. 31 C.F.R. § 103.18 (2001). The relevant portion of section 103.18 states:

Reports by banks of suspicious transactions.
(a) General. (1) Every bank shall file with the Treasury Department, to the extent and in the manner required by this section, a report of any suspicious transaction relevant to a possible violation of law or regulation . . . .
(2) A transaction requires reporting under the terms of this section if it is conducted or attempted by, at, or through the bank, it involves or aggregates at least $5,000 in funds or other assets, and the bank knows, suspects, or has reason to suspect that:
(i) The transaction involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities . . . as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;
(ii) The transaction is designed to evade any requirements of this part or of any other regulations promulgated under the Bank Secrecy Act;
While these provisions are extensive, they are not overly burdensome and are designed to obtain simply that information which, as the Secretary of the Treasury determined, "have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings."\footnote{325}

\section*{IX. The Patriot Act}

On October 26, 2001, the Patriot Act was signed into law.\footnote{326} While it was passed in a hurry, the groundwork for the legislation was in existence much earlier.\footnote{327}

The Act requires a number of things, but the provisions that primarily affect individuals are as follows:

- \textit{Section 312—Special due diligence for correspondent accounts and private banking accounts.}

This section requires each bank that opens or maintains a private banking or correspondent account in the United States for a foreign individual to "establish appropriate, specific, and, where necessary, enhanced due diligence polices, procedures, and controls that are reasonably designed to detect and report

\begin{itemize}
\item [(iii)] The transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction....
\end{itemize}

\textit{Id.}

\footnote{325. 31 C.F.R. § 103.15 (2001). For a summary of the BSA, see \textit{Information Technologies}, \textit{supra} note 7, at 35-39 for a summary of the BSA; \textit{see also} L. Richard Fischer, \textit{The Law of Financial Privacy} 4-2 - 4-4 (A.S. Pratt & Sons) (2001).}


\footnote{327. 147 CONG. REC. S10564 (daily ed. Oct. 11, 2001) (statement by Sen. Sarbanes) ("The modernization of our money laundering laws represented by Subtitle III [of the Patriot Act] is long overdue. It is not the work of one week or one weekend, but represents years of careful study and a bipartisan effort to produce a piece of prudent legislation."); \textit{see Minority Staff of the U.S. Senate Permanent Subcommittee on Investigations, Report on Correspondent Banking: A Gateway for Money Laundering} (Feb. 5, 2001), \textit{available at} http://www.senate.gov/~gov_affairs/psi_finalreport.pdf (last visited Feb. 28, 2002).}

instances of money laundering through those accounts." If a bank opens or maintains a private banking account for a foreigner, the bank must ensure that it takes "reasonable steps to ascertain the identity of the nominal and beneficial owners of, and the source of funds deposited into, such account as needed to guard against money laundering and report any suspicious transactions. . . ." If a bank opens or maintains a private banking account for a foreigner, the bank must ensure that it takes "reasonable steps to ascertain the identity of the nominal and beneficial owners of, and the source of funds deposited into, such account as needed to guard against money laundering and report any suspicious transactions. . . ."

The term "private banking account" is defined in the Act as an account that:

(i) requires minimum aggregate deposits of funds or other assets of not less than $1,000,000;
(ii) is established on behalf of one or more individuals who have a direct or beneficial ownership interest in the account; and
(iii) is assigned to, or is administered or managed by, in whole or in part, an officer employee, or agent of a financial institution acting as a liaison between the financial institution and the direct or beneficial owner of the account.

This section also requires that each bank that opens or maintains an account on behalf of "a senior foreign political figure" shall "conduct enhanced scrutiny of any such account" and shall take "reasonable steps . . . to detect and report transactions that may involve the proceeds of foreign corruption."

In light of its exclusive focus on large private banking accounts opened or maintained for foreigners and on the accounts of "senior foreign political figures," this section does not even affect United States customers. In addition, with regard to the

329. Id.
330. Id.
private banking accounts and the foreign political officials on which the section focuses, all that is required is for the bank to engage in enhanced due diligence and, as already required by law, to report suspicious activity. The need for caution in this area is clearly warranted in light of the issues raised regarding various high profile cases that involve corruption of foreign officials who have laundered their money through U.S. banks.

- **Section 314 - Cooperative efforts to deter money laundering.**

The primary aspect of this section which affects individuals is the authorization for banks to share information with one another, after notification to the Secretary of the Treasury, "regarding individuals, entities, organizations, and countries suspected of possible terrorist or money laundering activities." It should be stressed, however, that, as set forth in the Act, this ability to share information is limited to situations where notification has been made to the Secretary of the Treasury and where terrorism or money laundering is suspected. It does not authorize the dissemination of routine account or financial information or even the disclosure of information such as overdrafts in an account.

Another perspective on this provision is the fact that the many nationwide branches and offices of a large bank have access to the same account information within that bank system. If any

---


335. The dissemination of credit information, as authorized by the Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681u (2000), is more comprehensive than this narrowly tailored provision.
branches of such a bank were to close an account due to suspected money laundering, the bank’s other branches throughout the country would be aware of this information and would know to take extra precautions before opening another account for the same individual or company. Once the necessary procedures are satisfied, a bank in a small town will also be able to share similar concerns and warnings with the bank across the street. Even then, though, as mentioned above, the concerns must be limited to two specific areas—money laundering and terrorism.

- **Section 325—Concentration accounts at financial institutions.**

This section allows the Secretary of Treasury to issue regulations that would prohibit banks from allowing its customers to move their funds anonymously through concentration accounts.336 Further, the section states that if a bank does use a concentration account to commingle and transfer its customers’ funds, the bank must be able to document and trace the funds and identify what funds belong to which customer.337 The problem this section addresses is the situation that occurred at Citibank where an officer of the bank allowed Raul Salinas, the brother of the then President of Mexico, to transfer close to $100 million anonymously through the bank to various places such as the Cayman Islands, Switzerland, and London.338 This provision should not adversely affect the privacy rights of individuals; it simply prevents them from transferring sums of money anonymously through international channels.339


337. *Id.*


Section 326—Verification of Identification.

This section of the Act requires the Secretary of the Treasury to issue regulations that will set forth procedures for verifying the identity of customers seeking to open accounts at banks. The regulation will require "reasonable procedures" for verifying identity "to the extent reasonable and practicable." This section also provides for studies and recommendations for the "most timely and effective way to require foreign nationals to provide domestic financial institutions and agencies with appropriate and accurate information" concerning their identity.

In light of the fact that proper verification of identity at the time of account opening is a necessary and common practice, this requirement, which stresses the need for "reasonable procedures," should not create undue privacy concerns. In weighing privacy interests against those of the public, in general, and the banks, in particular, in safe and sound banking operations free from money laundering and fraud, it should be noted that the Financial Crimes Enforcement Network (FinCEN) SAR Activity Review of June 2001 cited identity theft as the number one trend in suspicious activities. FinCEN's updated SAR Activity Review, issued in October 2001, noted, in fact, that the instances of identity theft (as measured by the number of reports filed) had continued to increase from forty-four such reports in 1997 to 267 reports in 1999, to 637 reports in 2000, and to 332 reports for the first three months of 2001 (for an annualized amount in 2001 of 996 reports).

341. Id.
342. Id.
Section 351—Amendments relating to reporting of suspicious activities.

Section 355—Authorization to include suspicions of illegal activity in written employment references.

These two sections together provide for a safe harbor for banks, in response to requests for employment references, to provide information about the "possible involvement" of employees in "potentially unlawful activity." Prior to this time, banks could not take any steps to protect another bank from hiring an embezzler without the risk of being sued for slander, libel or violation of privacy. Even though a bank was required to report the "potentially unlawful activity" to the government, the bank had no protection if it reported the same information to another bank that was considering employing the person. The potential problem was that, even though the bank had filed a Suspicious Activity Report (SAR), all too often, in light of prosecutorial dollar thresholds, the low-level embezzler would not be prosecuted and would be able to proceed from one bank to another bank and to engage in fraud or embezzlement all over again.

A potential drawback to these two sections, however, is that no safe harbor exists for a bank that makes a disclosure pursuant to this authority "with malicious intent." While the intent of this provision is obvious and well-meaning, if "malicious intent" were construed to include the situation where the first bank intends to convince the second bank not to hire a person, that will be an obvious problem. In addition, even without such a strained interpretation, this provision could be very problematic since a disgruntled employee, fired for fraud or embezzlement, can easily allege some kind of vague or general malicious behavior on


347. The OCC has addressed this problem, in part, by putting into place a "fast-track" program whereby the agency considers bringing removal actions against insiders who were the subject of a SAR, were not prosecuted, but meet the grounds for a removal. U.S. DEPARTMENT OF THE TREASURY, OFFICE OF THE COMPTROLLER OF THE CURRENCY, POLICIES & PROCEDURES MANUAL 5310-8 (Subject: Fast Track Enforcement Program) (March 11, 1996) (available by request from the OCC). If the agency successfully removes these individuals from the industry through the use of its administrative powers under 12 U.S.C. § 1818(e) (2000), then the individual cannot, without regulatory permission, work in the banking industry. *Id.* at 4-5.
the part of the bank. Regardless of whether there is any validity to the claim, the bank will have to defend itself.\(^3\)

That process not only subjects the bank to needless and expensive litigation, but it also has the potential of discouraging a bank from giving an honest and frank employment reference in close cases.

- **Section 358—Bank secrecy provisions and activities of United States intelligence agencies to fight international terrorism.**

This section provides for an exception to the Right to Financial Privacy Act (RFPA).\(^4\) Specifically, the section amends the RFPA to allow for easier dissemination to the appropriate government agency of information pertaining to intelligence and counterintelligence relating to international terrorism.\(^5\) In light of the terrorist attacks on September 11, 2001, this provision is an understandable and supportable addition to the RFPA exceptions described below.

In summary, the Patriot Act provides helpful additions and amendments to the BSA, especially those provisions that support enhanced due diligence with regard to high-risk accounts, that restrict obviously high-risk transactions, and that allow for increased sharing between banks in order to better protect the industry to eliminate fraud. As set forth above, these provisions do not appear to unduly affect any privacy rights and are particularly important as demonstrated by the horrible terrorist attacks of September 11, 2001.

**X. GUIDELINES ON ANTI-MONEY LAUNDERING ENFORCEMENT**

In addition to the numerous pieces of legislation that compose the BSA,\(^6\) various organizations have issued numerous pieces of guidance which mirror and support the requirements of the BSA and the Patriot Act.

For instance, regarding account opening, the BSA requires that certain steps be taken to verify the identity of the customer,

\(^3\) See supra notes 127-251 and accompanying text (discussing the problem of a bank having to defend itself against baseless lawsuits).


\(^5\) Id.

\(^6\) See supra notes 302-10 and accompanying text.
including obtaining the customer's social security number. In addition, certain identifying information needs to be obtained when wire transfers over $3,000 are sent, or when a bank check is purchased with $3,000 or more in currency. Pursuant to Section 326 of the Patriot Act, the Secretary of the Treasury is to issue regulations that will set forth procedures for verifying the identity of customers seeking to open accounts at banks.

This emphasis on properly identifying customers is echoed by various industry issuances. Specifically, the Financial Action Task Force on Money Laundering (FATF), which issued a set of "Forty Recommendations" in June of 1996 to help combat international money laundering, addressed identification issues in a number of its recommendations. Among these recommendations are the following:

10. Financial institutions . . . should be required . . . to identify, on the basis of an official or other reliable identifying document, and record the identity of their clients, either occasional or usual, when establishing business relations or conducting transactions (in particular opening of accounts . . .).

In order to fulfill identification requirements concerning legal entities, financial institutions should, when necessary, take measures:

i. to verify the legal existence and structure of the customer . . .

ii. to verify that any person purporting to act on behalf of the customer is so authorised and identify that person.

355. The FATF was established by the “Group of Seven” at its economic conference in Paris in 1989. Fischer, supra note 325, at 4-16.
11. Financial institutions should take reasonable measures to obtain information about the true identity of the persons on whose behalf an account is opened or a transaction conducted. . . . 357

Similarly, the Basel Committee on Banking Supervision issued guidance in October, 2001 on Customer due diligence for banks, which also emphasizes the importance of obtaining the true identity of the customer. 358 In that publication, the Basel Committee notes the following:

1. Supervisors around the world are increasingly recognising the importance of ensuring that their banks have adequate controls and procedures in place so that they know the customers with whom they are dealing. Adequate due diligence on new and existing customers is a key part of these controls. Without this due diligence, banks can become subject to reputational, operational, legal and concentration risks, which can result in significant financial cost.

20. Banks should develop clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher than average risk to a bank. In preparing such policies, factors such as customers' background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators should be considered. . . .

22. Banks should establish a systematic procedure for identifying new customers and should not

357. Id.

establish a banking relationship until the identity of a new customer is satisfactorily verified.

23. The best documents for verifying the identity of customers are those most difficult to obtain illicitly and to counterfeit. . . .

27. Banks need to obtain all information necessary to establish to their full satisfaction the identity of each new customer and the purpose and intended nature of the business relationship. . . .

The need for care is especially great in private banking due to the high risk nature of these accounts. It is for this reason that Section 312 of the Patriot Act requires that banks "establish appropriate, specific, and, where necessary, enhanced due diligence polices, procedures, and controls that are reasonably designed to detect and report instances of money laundering through those accounts" when foreigners open private bank accounts. When a bank opens or maintains a private banking account for a foreigner, the bank must take "reasonable steps to ascertain the identity of the nominal and beneficial owners of, and the source of funds deposited into, such account. . . ." Accordingly, the Basel Committee provided the following guidance:

25. Banks that offer private banking services are particularly exposed to reputational risk, and should therefore apply enhanced due diligence to such operations. . . . All new clients and new accounts should be approved by at least one person, of appropriate seniority, other than the private banking relationship manager.

359. Id. at 1-11.
360. See supra notes 333 and 338 and accompanying text.
362. Id.
363. BASEL GUIDANCE, supra note 358, at 11.
In addition, a new group composed of eleven of the world's largest banks and Transparency International, a global anti-corruption organization, issued guidance on October 30, 2000, called the "Global Anti-Money-Laundering Guidelines for Private Banking—Wolfsberg AML Principles" addressing just private banking.\(^\text{364}\) Part of the guidance provided the following:

The bank will endeavor to accept only those clients whose source of wealth and funds can be reasonably established to be legitimate.\(^\text{365}\)

Beneficial ownership must be established for all accounts. Due diligence must be done on all principal beneficial owners.\(^\text{366}\)

It is essential to collect and record information covering the following categories:

- Purpose and reasons for opening the account;
- Anticipated account activity;
- Source of wealth (description of the economic activity which has generated the net worth);
- Estimated net worth;
- Source of funds (description of the origin and the means of transfer for monies that are accepted for the account opening); and
- References or other sources to corroborate reputation information where available.\(^\text{367}\)

The Wolfsberg principles also indicate that additional due diligence should be required when any of the following are involved:


\(^{365}\) Id. § 1.1.

\(^{366}\) Id. § 1.2.2.

\(^{367}\) Id. § 1.3.
- Numbered accounts;
- High-risk countries;
- Offshore jurisdictions;
- High-risk activities; or
- Public officials.\textsuperscript{368}

With respect to dealing with public officials, the Wolfsberg principles state: "Individuals who have or have had positions of public trust such as government officials, senior executives of government corporations, politicians, important political party officials, etc. and their families and close associates require heightened scrutiny."\textsuperscript{369} The risk of banks receiving funds from corrupt officials, of course, is part of the focus of Section 312 of the Patriot Act which requires "enhanced scrutiny" of accounts maintained by a "senior foreign political figure."\textsuperscript{370} The concern about foreign corrupt officials laundering their money was also the focus of the Treasury guidance issued in January, 2001.\textsuperscript{371} The Basel Committee touched on the issue in the following way:

41. Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose a bank to significant reputational and/or legal risks. . . \textsuperscript{372}

The existence of these various pronouncements by industry and international groups clearly underscores the support and need for strong anti-money laundering enforcement measures. However, as Treasury Deputy Secretary Dam recently testified, there is always a balancing issue to address:

We acknowledge, as we must, that now more than ever law enforcement and the intelligence community must have the ability to obtain and share financial information. However, that need must

\textsuperscript{368} Id. § 2.
\textsuperscript{369} Id. § 2.5.
\textsuperscript{371} See supra note 332.
\textsuperscript{372} BASEL GUIDANCE, supra note 358, at 14.
always be balanced against our fundamental notions of privacy. Striking that balance is the challenge for Treasury as we implement this legislation.  

Consequently, it is necessary to closely review the requirements of the privacy statutes, in particular, the RFPA, and to explore whether its protections are sufficient while not impeding necessary anti-money laundering enforcement procedures.

XI. THE RIGHT TO FINANCIAL PRIVACY ACT

"The centerpiece of federal statutory efforts to protect individual privacy is the federal Right to Financial Privacy Act of 1978."374 In general, "the RFPA prohibits financial institutions from disclosing a customer's financial records to the federal government except in limited circumstances such as pursuant to the customer's authorization, an administrative subpoena or summons, a search warrant, a judicial subpoena, or a formal written request in connection with a legitimate law enforcement inquiry, or to a supervisory agency in connection with its supervisory, regulatory, or monetary function."375 Specifically, the RFPA has three basic purposes:

(1) to require that customers be notified before disclosure of their records to the government; (2) to give customers standing to challenge release of their records to the government; and (3) to require government agencies to produce a "paper trail" documenting the disclosure of customer information to the government, as well as any interagency transfer of such information.376

374. FISCHER, supra note 325, at 2-1. While there are many other privacy statutes, this paper will only focus on the RFPA due to its relevance to the disclosure of customers' financial information to the federal Government.
376. FISCHER, supra note 325, at 2-3.
The specific provisions of the RFPA include the following:

- **12 U.S.C. § 3401—Definitions.**

  This definitional section is important in that it limits the scope of the RFPA to individuals and to partnerships of five or fewer people.\(^{377}\)

- **12 U.S.C. § 3402—Access to financial records by government authorities prohibited; exceptions.**

  This section sets out the basic premise that the federal government cannot obtain access to any records of a financial institution unless in accordance with one of the exceptions contained in the RFPA.

- **12 U.S.C. § 3403—Confidentiality of financial records.**

  This section sets out the reverse premise that no financial institution can provide bank records to the federal government unless in accordance with the provisions of the RFPA.\(^{378}\) In addition, this section requires a certification from the government seeking records to the effect that it has complied with the applicable provisions of the RFPA.\(^{379}\)

  However, this section allows for a financial institution to notify the government that it has information relevant to a possible violation of law, and allows the bank to provide the government with identifying information concerning the individual and the account involved as well as an explanation of “the nature of [the] suspected illegal activity.”\(^{380}\) This provision also contains a safe harbor for the financial institution.\(^{381}\)

---


\(^{378}\) Id. § 3403(a).

\(^{379}\) Id. § 3403(b).

\(^{380}\) Id. § 3403(c).

\(^{381}\) Id.
- **12 U.S.C. § 3404—Customer authorizations.**

  This section provides for customers to authorize disclosure.\(^{382}\) Importantly, the statute indicates that authorization cannot be required as a condition to doing business.\(^{383}\)

- **12 U.S.C. § 3405—Administrative subpoena and summons.**

  This provision indicates that the federal government can obtain financial records pursuant to an administrative subpoena if: (a) "there is reason to believe that the records sought are relevant to a legitimate law enforcement inquiry"; (b) a copy of the subpoena has been served on the customer ten days prior to the return date for the subpoena; and (c) the customer has not contested the subpoena pursuant to procedures set out in the RFPA.\(^{384}\)

- **12 U.S.C. § 3406—Search warrants.**

  This section permits the federal government to obtain financial records with the use of a search warrant obtained pursuant to the Federal Rules of Criminal Procedure.\(^{385}\) However, an after-the-fact notice has to be sent to the customer within 90 days, or after a longer period of time if authorized by a court.\(^{386}\)

- **12 U.S.C. § 3407—Judicial subpoena.**

  This section allows for the use of a court subpoena, with the same three step requirements as set out for administrative subpoenas under 12 U.S.C. § 3405.

- **12 U.S.C. § 3408—Formal written request.**

  This section allows for the federal government to file a formal written request for the financial records, if it cannot obtain

---

382. Id. § 3404(a).
383. Id. § 3404(b).
386. Id. § 3406(b)-(c).
an administrative or judicial subpoena. The request must be authorized by the particular agency's regulations, and the request must be based on a "reason to believe that the records sought are relevant to a legitimate law enforcement inquiry." A copy of the request must be sent to the customer who can contest the dissemination of the records, but only if the customer files a motion with the court swearing that the records are not relevant to the stated legitimate law enforcement inquiry or setting forth other legal objections.

- **12 U.S.C. § 3409—Delayed notice.**

  This section allows for a court sanctioned delay in the procedures for providing notice to the customer.

- **12 U.S.C. § 3412—Use of information.**

  This section allows for the agency receiving information pursuant to the RFPA to transfer it to another agency upon certifying in writing that there is reason to believe that the records are relevant to a legitimate law enforcement inquiry by the receiving agency. If such a transfer is made, however, a formal notification has to be made to the customer within 14 days, unless a delay is sanctioned by a court.

  This section, however, specifically allows for transfers, without notification to the customer, of information between supervisory agencies, defined to mean the banking regulatory agencies, the SEC, the CFTC and, with regard to BSA related matters, the Department of the Treasury. In addition, the section allows for a transfer, without notification to the customer, of financial records from any agency to the Department of Justice or to the Department of the Treasury if the transferring agency certifies that there is reason to believe that the records may be relevant to a violation of federal criminal law and the records were

---

387. *Id.* § 3408(a)(3).
388. The Fifth Amendment concerns that such a requirement might raise are beyond the scope of this paper. It should be noted that the procedure for customer challenges under 12 U.S.C. § 3410 is similar.
389. *Id.* § 3412(a).
390. *Id.* § 3412(b).
obtained by the agency in the exercise of its supervisory or regulatory functions. 391


This section provides the following very crucial exceptions to the scope of the RFPA:

- Access to financial records by the banking regulatory agencies. 392
- Disclosure of financial records under the tax code (Title 26). 393
- Disclosure of financial records pursuant to any federal statute or regulation. 394
- Disclosure of financial records in administrative, civil or criminal cases in which the government and the customer are both parties. 395
- Disclosure of the name, address, account number and type of account for a legitimate law enforcement inquiry in connection with a financial transaction or class of financial transactions or in connection with a foreign country where the government is exercising financial controls over foreign accounts relating to that country. 396
- Disclosure of financial records pursuant to a grand jury subpoena. 397
- Disclosure of financial records to the General Accounting Office in connection with an inquiry directed at a government entity. 398

391. Id. § 3412(f).
392. Id. § 3413(b).
393. Id. § 3413(c).
395. Id. § 3413(e).
396. Id. § 3413(g).
397. Id. § 3413(i).
398. Id. § 3413(j).
Disclosure of financial records of an employee, officer or director of any financial institution or any major customer acting in concert with such an individual in connection with any possible crime against the financial institution or a violation of the BSA.\(^{399}\)


This section provides for the following additional exceptions to the RFPA:

- Disclosure of financial records to a government agency authorized to conduct foreign intelligence or counter intelligence activities.\(^{400}\)
- Disclosure of financial records to a government agency authorized to conduct investigations or intelligence or counter-intelligence analysis related to international terrorism.\(^{401}\)

While these sections of the RFPA are very extensive, they at least set out with precision when and how a financial institution can hand records over to the federal government. However, the Act has historically been controversial among the banking regulatory and law enforcement agencies that have primarily criticized the customer notification provisions of the Act:\(^{402}\)

It is very difficult to quantify the effect to which the RFPA has actually impeded an investigation or to what extent a lack of information influenced a decision to not pursue a case. We do know, however, that the limitations, actual or perceived,

---

399. Id. § 3413(l).
401. This provision was added by § 358 of the Patriot Act. See Patriot Act, Pub. L. No. 107-56, § 358 (2001).
have unreasonably hindered full cooperation among and between the banking agencies and the law enforcement community. The Justice Financial Institutions Regulatory Working Group in the final Agreement of April 2, 1985, unanimously concluded that restraints like the RFPA should be modified if the Government is to coordinate effectively its efforts in its battle against all types of crime. We have long maintained that these limitations could be significantly relaxed without any significant invasion into privacy rights. . . . 403

However, since the time of this testimony, various amendments were made to the RFPA, including the exception in 12 U.S.C. § 3412(f) allowing for transfer of documents to the Department of Justice and to the Department of Treasury without notification to the customer, and the exception in 12 U.S.C. § 3413(1) allowing for the production of documents pertaining to an insider suspected of engaging in a crime against the financial institution or engaging in money laundering.

The primary effect of the RFPA was to prohibit the informal transfer of bank records to law enforcement agencies that was complained about in Burrows 404 and Suburban, 405 but was permitted in Chapman 406 and Miller. 407 While compliance with requirements under the RFPA for formal requests and written certifications can be cumbersome and occasionally unwieldy and time-consuming, it provides certainty to the banks and a degree of protection to the customer. In addition, the various exceptions that have been factored into the RFPA, including the exceptions for transferring documents to the Department of Justice and the


Department of Treasury without notification to the customer;\textsuperscript{408} responding to grand jury subpoenas without notification to the customer,\textsuperscript{409} and allowing for the transfer of documentation pertaining to bank insiders without notification,\textsuperscript{410} all facilitate the proper and necessary flow of information to law enforcement agencies while still imposing restrictions that protect the interests of the customer. In addition, the primary method of providing appropriate information to law enforcement agencies—through the filing of a formal SAR—is protected under the RFPA and does not require notification to the customer.\textsuperscript{411}

\textbf{XII. CONCLUSION}

While the issue of privacy rights is a sensitive and controversial topic, the legislature, with the support of most of the recent court cases, has made a good effort to establish an appropriate balance between privacy rights—as set forth primarily in the RFPA—and the need for strong and effective anti-money laundering enforcement efforts—through the BSA and the various exceptions to the RFPA. However, this is a developing and changing area. The Patriot Act, for instance, as a new piece of legislation, reflects the changing environment, clearly affecting the dynamics of the area, but not drastically altering individuals’ privacy rights.

As Samuel D. Warren and Louis D. Brandeis said over 100 years ago:

\begin{quote}
That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new
\end{quote}

\begin{footnotesize}
\begin{enumerate}
  \item Id. § 3413(i).
  \item Id. § 3413(i).
\end{enumerate}
\end{footnotesize}
rights, and the common law, in its eternal youth, grows to meet the demands of society.\textsuperscript{412}

The extent of privacy rights has changed considerably since the early cases, as reflected by such cases as \textit{Olmstead}.\textsuperscript{413} In addition, the statutory landscape, with such pieces of legislation as the BSA and the RFPA (which themselves have been amended and altered a number of times), is reflective of the developments and changes over time.

It is also reflective of the continuing tension in this area. The banking agencies' "Know Your Customer" (KYC) proposal, issued on December 7, 1998\textsuperscript{414} and withdrawn on March 29-30, 1999,\textsuperscript{415} underscored this tension.\textsuperscript{416} Even though some commentators have noted that the "public opposition [to the proposed regulation] probably was an overreaction,"\textsuperscript{417} it is clear that the tensions and concerns exist.

These tensions and concerns resulted in a rejection of the agencies' proposed KYC regulation three years ago.\textsuperscript{418} However, recent events and further analysis resulted in the passage of the Patriot Act, which requires regulations setting forth procedures for


\textsuperscript{413} \textit{Olmstead v. United States}, 277 U.S. 438 (1928).


\textsuperscript{416} David F. Scranton, \textit{Public cried 'no' to know-your-customer regulations}, \textit{NAT'L L.J.}, May 10, 1999, at B5 ("News reports indicated that more than 300,000 comments were submitted and that extraordinarily few were positive. The agencies reported that most comments reflected public concern over the privacy of the information that would be collected and held by financial institutions. . . .").

\textsuperscript{417} Id. In spite of the negative comments, many from individual banks, the banking industry as a whole has acknowledged that a KYC program is important for a bank to have. In this regard, in commenting on proposed regulations under the Patriot Act, the New York Clearing House, in a letter endorsed by the American Bankers Association, said that KYC policies and procedures are "the foundation of an effective anti-money laundering program." Letter from the New York Clearing House, to the Office of the Assistant General Counsel (Enforcement) of the Department of the Treasury, Feb. 11, 2002, at 9-10. This comment again underscores the differing views on this issue and the fact that the final word has not yet been heard.

\textsuperscript{418} See supra note 415 and accompanying text.
verifying the identity of customers seeking to open accounts at banks.\textsuperscript{419} While the Patriot Act does not require regulations that are as extensive as the proposed KYC regulation\textsuperscript{420}—in that the Patriot Act regulations are not designed to address on-going review or monitoring of accounts\textsuperscript{421}—the requirement to ensure "reasonable procedures" for verifying the identity of customers opening accounts\textsuperscript{422} is a strong statement of the need for banks to verify, or know, the identity of their customers. It is also a strong reflection of the changes that can, and mostly will continue to, occur in this area.

While the Patriot Act and the international guidance set forth above reflect the need for continued changes and for strengthening anti-money laundering efforts, especially in the area of account identification procedures and in curtailing risks relating to certain high profile accounts and transactions, the true extent of what the public, the courts, and the legislature will deem to be an acceptable balance will continue to evolve.

\textsuperscript{419} See supra note 341 and accompanying text.
\textsuperscript{420} Id.
\textsuperscript{421} See supra note 414 and accompanying text.
\textsuperscript{422} See supra note 341 and accompanying text.