Contracting for Financial Privacy: The Rights of Banks and Customers Under the Reauthorized Patriot Act

*Aditi A. Prabhu**

ABSTRACT

The 2001 Patriot Act chipped away financial privacy protections by allowing law enforcement authorities easier access to bank customer records. Under the Patriot Act, federal authorities may access customer records by issuing formal subpoena-like requests under the Foreign Intelligence Surveillance Act ("FISA") or informal national security letters ("NSLs") to banks while prohibiting notice to any affected customers. However, the 2006 revisions to the Patriot Act permit banks to challenge FISA requests and NSLs in federal court before releasing customer records. While the Act does not require banks to make these challenges on behalf of their customers, this Article will argue that the contracts banks sign with their customers—interpreted in light of the banking tradition of confidentiality and the current regime of federal and state privacy protections—obligate banks to review government requests for customer records and file challenges when appropriate. Furthermore, I will argue that banks and customers should be able to enter into contracts explicitly obligating banks to challenge FISA requests and NSLs and that such contracts would be enforceable and financially feasible.

*Aditi Prabhu graduated from Harvard College in 2004 with an A.B. in Biology and from Yale Law School in 2007.

I. INTRODUCTION

On March 9, 2006, President George W. Bush signed into effect the USA Patriot Improvement and Reauthorization Act of 2005 (hereinafter "Reauthorized Patriot Act").[1] Among the many subtle modifications to the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) (hereinafter "Patriot Act of 2001" or "original Patriot Act"), the Reauthorized Patriot Act gives a small nod to financial privacy—a seeming check on the government's power to obtain bank records without providing customers any notice or the opportunity for a hearing. Although the Reauthorized Patriot Act still allows the Federal Bureau of Investigation ("FBI") to request the production of customers' books and records from financial institutions, a new provision allows the recipient institution to challenge these requests.[2] Whether this concession heralds an era of enlarged customer privacy rights wholly depends on whether financial institutions seize the opportunity to defend their customers' records from intrusive government searches.

This Article will argue that the newly created right of banks to challenge law enforcement inquiries should be construed as a duty rather than a privilege: once empowered, banks are obliged to screen requests for records and file petitions in opposition, at least under certain circumstances. Although the text of the Reauthorized Patriot Act does not explicitly create enforceable rights for customers, its provisions do not operate in a vacuum.[3] Instead, banks confront exogenous sources of obligations that should inform their decision of whether to challenge law enforcement inquiries.[4] Although Supreme Court precedent indicates that customers enjoy only limited constitutional protection of privacy rights in financial information

1. Press Release, Office of the Press Secretary, President Signs USA PATRIOT Improvement and Reauthorization Act (Mar. 9, 2006), *available at* http://www.whitehouse.gov/news/releases/2006/03/20060309-4.html.

2. 50 U.S.C.A § 1861(f)(2)(A)(i) (West. Supp. 2007) ("A person receiving a production order may challenge the legality of that order by filing a petition with the pool established by section 1803(e)(1) of this title.").

3. *See infra* Part III (illustrating that the Reauthorized Patriot Act must be viewed in the proper historical context, which includes Congress' attempts to heighten customer protections by passing the Right to Financial Privacy Act and the Gramm-Leach-Bliley Act).

4. *See infra* Part III.C (explaining that banks have at least an implied contractual duty of confidentiality to their customers, if not an explicit duty created by contractual language, and that this duty should help banks decide whether or not to challenge a law enforcement's inquiry into a customer's financial information).

voluntarily conveyed to banks,[5] a patchwork of federal statutory schemes speak to the importance of protecting financial information from unwarranted distribution.[6] These federal rights are bolstered by state constitutional and statutory protections.[7] Furthermore, customers are endowed with contractual rights from the arrangements they enter into with financial institutions to which they reveal private and sensitive information. These rights are embedded in both the privacy agreements signed by banks and their customers and in the expectations created by the nature of the relationship and the customs of the banking industry.[8]

In addition, this Article proposes that banks and customers could explicitly require banks to challenge law enforcement inquiries, including subpoenas, through clear duty-creating contractual language.[9] It explores the costs of following through with this obligation given the frequency of law enforcement inquiries and the costs of raising petitions.[10] Finally, this Article examines whether there would be market demand for these additional privacy protections.[11]

II. REAUTHORIZED PATRIOT ACT

In passing the Patriot Act of 2001, "Congress set certain more controversial provisions to sunset at the end of 2005, at which time Congress would be able to use the experience of the intervening four years to devise what changes might be necessary."[12] Hence, Congress

5. *See infra* Part III.A (showing that the Supreme Court, in *Katz v. United States*, 389 U.S. 347, 359 (1967), refused to find a general right to privacy in the Fourth Amendment and that, in *United States v. Miller*, 425 U.S. 435, 443 (1976), the Court held that the search and seizure of bank records is not a violation of the Fourth Amendment).

6. *See infra* Part III.B (explaining that Congress passed the Right to Financial Privacy Act in order to protect customers from unwarranted intrusions into their bank records).

7. *See infra* Part III.B.3 (stating that states such as Colorado, Illinois, Florida, Lousiana, Marlyland, New Hampshire, and Alabama have taken constitutional or statutory measures to protect customers' privacy of financial information).

8. *See infra* Part III.C (arguing that many contracts between banks and customers contain an explicit duty of confidentiality in the contract and in the bank-customer relationship itself because the relationship transcends that of a mere creditor-debtor relationship).

9. *See infra* Part V.A (proposing that the Reauthorized Patriot Act should allow banks and customers to explicitly contract for assurance that banks will challenge the government's requests for a customer's financial records).

10. *See infra* Part VI (using a cautious estimation in order to show that the cost to bank customers for such protection would be minimal).

11. *Id.* (arguing that the market for these protections exists among the 150 million bank customers in the United States).

12. Viet D. Dinh & Wendy J. Keefer, *FISA and the PATRIOT Act: A Look Back and A Look Forward*, 35 GEO. L.J. ANN. REV. CRIM. PROC. iii, iv (2006) [hereinafter Dinh]; Charles Doyle, *USA Patriot Act: Provisions That Expire on December 31, 2005*, CRS Report for Congress at 2 (Jan. 2, 2004) ("Thereafter, the authority remains in effect only as it relates to foreign intelligence

reconsidered much of the Patriot Act of 2001 in drafting the Reauthorized Patriot Act. This Article will focus solely on amendments to the original Patriot Act that implicate financial privacy in the investigative context. This Part compares three types of requests for records of decreasing formality—FISA requests, mandatory national security letters, and non-mandatory national security letters—on the basis of their historical origins, pre-enforcement safeguards, and post-issuance opportunities for judicial review.

A. Access to Records under Amendments to FISA

As discussed above, the Reauthorized Patriot Act permits banks to challenge government requests for customer records.[13] The statutory authorization for this newly conferred power comes from amendments to the Foreign Intelligence Surveillance Act ("FISA")[14], which gives the FBI the power to issue confidential requests for financial records.[15] Notably, Congress originally passed FISA in 1978 to bring greater congressional oversight to counterterrorism operations.[16] The Act, which reflected a concern that the FBI, Central Intelligence Agency ("CIA"), and Department of Defense ("DoD") abused their powers during the preceding decades, constituted a departure from the independence that agencies charged with protecting national security had originally enjoyed.[17] In particular, FISA set boundaries on the use of electronic surveillance and subjected counterintelligence activities to judicial supervision.[18] Under the FISA framework, FBI agents were permitted to conduct electronic searches and physical searches only

investigations begun before sunset or to offenses or potential offense [sic] begun or occurring before that date.").

13. 50 U.S.C.A. § 1861(f)(2)(A)(i) (West Supp. 2007); *see supra* text accompanying note 2.

14. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95–511, 92 Stat. 1783 (1978).

15. 50 U.S.C. §§ 1801–1862 (2000 & Supp. II 2002).

16. *See* Michael J. Woods, *Counterintelligence and Access to Transactional Records: A Practical History of USA PATRIOT Act Section 215*, 1 J. NAT'L SEC. L. & POL'Y 37, 40 (2005) [hereinafter Woods] (citing Richard A. Best, Jr., *Proposals for Intelligence Reorganization 1949–2004* (Cong. Res. Serv. RL32500) (Jul. 29, 2004), at 17–25) (stating that Congress was prompted to control counterintelligence activities because of abuse by the FBI, CIA, and Department of Defense during the 1960s and 1970s).

17. Woods, *supra* note 16, at 40 ("The revelation of abuses by the FBI, CIA, and DoD during the 1960s and 1970s, however, prompted Congress to bring counterintelligence activities under a higher degree of regulation.").

18. William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 74–77 (2001).

after using information gathered by less intrusive techniques to satisfy the probable cause standard.[19]

FISA not only reined in the previously unchecked authority of these agencies by statute but also spurred societal awareness of the tenuous balance between the powers granted to law enforcement and the protections retained for civil liberties. As Michael J. Woods, the former chief of the FBI's National Security Law Unit and the Principal Legal Advisor to the National Counterintelligence Executive, reflects: "One legacy of this period of regulation was an enduring concern that the tools available to counterintelligence should not be used to subvert the constitutional protections of criminal law."[20] To address this concern, FISA created "a 'wall,' built of legal and policy requirements and reinforced by culture, which separated counter-intelligence officers from criminal investigators."[21]

This "wall" lasted until 2001 when it was dismantled by the Patriot Act of 2001. The Patriot Act of 2001 amended FISA to allow the FBI to request individual financial records in the course of antiterrorism investigations[22] and prohibited financial institutions from notifying their customers of any such requests.[23] This provision was among the most contentious extensions of federal law enforcement authority in the original Patriot Act. As Woods speculates, "[p]erhaps no provision of the Act has generated more controversy than § 215, which authorizes the FBI to seek a court order compelling the production of 'any tangible things' relevant to certain counterintelligence and counterterrorism investigations."[24]

Under section 215, the FBI can obtain customer financial records by applying to a district judge for an order requiring the financial institution to produce tangible things including records.[25] In reviewing the application, the judge must determine whether the application meets the statutory criteria, namely a factual showing of reasonable grounds,

19. Woods, *supra* note 16, at 41 (stating that such less intrusive means include interviews, publicly available information and "surveillance in areas where no reasonable expectation of privacy exists").

20. *Id.* at 40.

21. *Id*.

22. 50 U.S.C.A. § 1861(a) (West 2004 & Supp. 2007).

23. 50 U.S.C.A. § 1861(d) (West 2004 & Supp. 2007); President Signs USA PATRIOT Improvement and Reauthorization Act, *supra* note 1 ("Before the Patriot Act, criminal investigators were often separated from intelligence officers by a legal and bureaucratic wall.").

24. Woods, *supra* note 16, at 37 (quoting Pub. L. No. 107–56, § 215, 115 Stat. 272, 287–88 (codified at 50 U.S.C. §§ 1861–1862 (Supp. II 2002))).

25. 50 U.S.C.A. § 1803(a) (West 2004) (designating judges to review applications for and granting orders approving electronic surveillance).

compliance with so-called minimization procedures, and general lawfulness.[26] If the judge concludes that the application satisfies these requirements, the judge shall enter an ex parte order approving the release of tangible things.[27] The production order imposes a duty of nondisclosure on the party requested to release the records. The duty of nondisclosure is mitigated by a few narrowly construed statutory exceptions, namely permission to speak to others as necessary to comply with the order and to a lawyer in order to obtain legal advice.[28]

Tucked into the Reauthorized Patriot Act is a provision empowering the institution from which records are solicited to challenge the production order by granting judicial review of such challenges by a specified pool of FISA court judges.[29] While providing financial and other record-keeping institutions with the power to challenge subpoenas, the Reauthorized Patriot Act does not explicitly require the institutions to exercise this option.[30] On the contrary, the Reauthorized Patriot Act pronounces: "A person who, in good faith, produces tangible things under an order pursuant to this Part shall not be liable to any other person for such production."[31] However, the language is not necessarily determinative on the question of institutional duty or liability to customers. Even if banks may not be held liable for their actual disclosures, their failure to challenge the request in light of the background system of obligations and expectations preceding the Reauthorized Patriot Act may be an independent basis for a procedural injury.

B. National Security Letters

Along with the formal mechanism described above, investigative agencies may also issue National Security Letters ("NSLs"), which do not require pre-enforcement approval by a judicial officer. Under the NSL process, the agency director may request a financial institution to

26. 50 U.S.C.A. § 1861(f)(2)(B) (West Supp. 2007) (allowing a judge to grant a petition to modify or set aside a production order only if the order does not meet the requirements of this section or is otherwise unlawful); H.R. REP. NO. 109–333, at 91 (2005) (Conf. Rep.), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_reports&docid=f:hr333.109.pdf. [hereinafter H.R. REP. NO. 109–333].

27. 50 U.S.C.A. § 1861(c)(1) (West 2004 & Supp. 2007).

28. 50 U.S.C.A. § 1861(d)(1)(A), (B) (West Supp. 2007).

29. H.R. REP. NO. 109–333, *supra* note 26, at 91 (discussing section 106); 50 U.S.C.A. § 1861(f)(2)(A)(i) (West Supp. 2007) ("The person receiving the production order may challenge the legality of that order by filing a petition with the pool established by § 1803(e)(1).").

30. 50 U.S.C.A. § 1861(f)(2)(A)(i) (West Supp. 2007) (providing that the recipient of a request for records "may challenge" its legality).

31. 50 U.S.C.A. § 1861(e) (West 2004).

produce records by "certif[ying] in writing to the financial institution that such records are sought for foreign counter intelligence purposes to protect against international terrorism or clandestine intelligence activities."[32] Congress granted agencies charged with protecting national security the power to issue NSLs in order to allow counterintelligence agents to obtain transactional information about investigative suspects.[33] When Congress first permitted these agencies to issue NSLs, it abstained from requiring the recipients of the letters to comply.[34] Until 1986, it was left to the discretion of the institution whether to release the requested records on a case by case basis.[35] In 1986, Congress mandated that financial institutions comply with NSL requests for records.[36] However, compliance was only mandatory for the narrow set of record requests where "there [were] specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains [was] or may [have been] a foreign power or an agent of a foreign power."[37] In 1993, this requirement was reduced to "a connection with a suspected intelligence officer or suspected terrorist or other indication of spying."[38] The Patriot Act of 2001 promulgated an even more lenient standard, requiring only "relevance to an investigation of international terrorism or clandestine intelligence activities."[39]

In contrast to the FISA requests described above in Part II.A, the NSL issuance process involves few procedural safeguards to balance individual privacy against competing governmental interests.[40] In a

32. 12 U.S.C.A. § 3414(a)(5)(A) (West 2001 & Supp. 2004).

33. Woods, *supra* note 16, at 41 (defining transactional information as "information that broadly describes information that documents financial or communications transactions without necessarily revealing the substance of those transactions," and listing examples of such transactional information as records of bank accounts and money transfers).

34. H.R. REP. NO. 99–690(I), at 16 (1986), *reprinted in* 1986 U.S.C.C.A.N. 5327, 5342.

35. Intelligence Authorization Act for Fiscal Year 1987, Pub. L. No. 99–569, § 404, 100 Stat. 3190, 3197 (1986).

36. *Id.*

37. S. REP. NO. 99–307, at 19 (1986).

38. Dinh, *supra* note 12, at xx (citing 18 USC § 2709(b) (2000 & Supp. III 2003)).

39. *Id.*; Jeffrey Rosen, *Who's Watching the FBI?*, N.Y. TIMES MAG., Apr. 15, 2007, *available at* http://www.nytimes.com/2007/04/15/magazine/15wwlnlede.t.html?ref=magazine ("The F.B.I. could issue the letters only if senior officials in Washington had a factual basis for believing that the records pertained to a suspected spy or terrorist. But the Patriot Act diluted these requirements, allowing F.B.I. field agents to issue the orders on their own say-so merely by asserting that they were 'relevant' to a terrorism investigation.").

40. *E.g.*, 12 U.S.C.A. § 3414(b)(1) (West 2001 & Supp. 2007) (explaining that the government will not be prevented from getting the financial records if it determines that delay would create immediate danger of physical injury to any person, serious property damage, or flight to avoid prosecution).

recent journalistic investigation uncovering the widespread use of the letters, the *New York Times* reported that "[a]s an investigative tool, the letters present relatively few hurdles; they can be authorized by supervisors rather than a court."[41] Furthermore, there is no formal mechanism, such as judicial review, before a request is issued to assure that requests are narrowly tailored and limited to the records of those individuals for whom there is some reasonable basis for suspicion.[42] One reporter observed that the "[p]assage of the Patriot Act in October 2001 lowered the standard for issuing the letters, requiring only that the documents sought be 'relevant' to an investigation and allowing records requests for more peripheral figures, not just targets of an inquiry."[43]

Financial institutions may challenge NSLs by a process parallel to that for requests under FISA. The recipient of the request for records may petition the district court to modify or set aside the nondisclosure requirement associated with the request.[44] In addition, the Committee Report accompanying the Reauthorized Patriot Act emphasized that the reworded provision authorizing bank challenges "makes explicit that the recipient of a national security letter (NSL) may consult with an attorney and challenge the NSL in court."[45] In evaluating such a challenge, the court's standard of review is narrow and deferential: the court may set aside the nondisclosure requirement or otherwise modify the NSL only if it finds that there is no reason to believe that such changes would endanger national security.[46] Even in light of such a finding by the court, a high-ranking FBI official may "certify" that the disclosure would pose a danger, and this certification will be treated as

41. Eric Lichtblau & Mark Mazzetti, *Military Expands Intelligence Role in U.S.*, N.Y. TIMES, Jan. 14, 2007, *available at* http://www.nytimes.com/2007/01/14/washington/14spy.html?ei=5070&en=efff109ec71ce18b&ex=1187582400&adxnnl=1&adxnnlx=1187453401-WIf621Y6iQwAsauubXFQ [hereinafter Lichtblau]; Rosen, *supra* note 39 ("In March, a report by the inspector general of the Justice Department described 'widespread and serious misuse' of national security letters after the U.S.A. Patriot Act of 2001 significantly expanded the F.B.I.'s authority to issue them: between 2003 and 2005, he concluded, the F.B.I. issued more than 140,000 national security letters, many involving people with no obvious connections to terrorism.").

42. *See generally* 50 U.S.C.A. § 1804 (West 2004 & Supp. 2007) (listing requirements for an order).

43. Lichtblau, *supra* note 41.

44. 18 U.S.C.A. § 3511(b) (West Supp. 2007).

45. H.R. REP. NO. 109–333, *supra* note 26, at 95.

46. *See id.* (saying that a court may modify or set aside such a nondisclosure requirement if it finds that there is no reason to believe that disclosure may harm national security; interfere with criminal, counterintelligence, or counterterrorism investigations; interfere with diplomatic relations; or endanger the life or physical safety of a person).

conclusive unless the court finds that it was made in bad faith.[47] If the entity does not comply with the request for production following an unsuccessful challenge, the Attorney General may invoke the district court to issue an order requiring compliance.[48] If the entity fails to obey the order, it may be held liable for contempt of court.[49]

The availability of pre-enforcement judicial review of NSLs is essential to the constitutionality of the process.[50] As in the case of administrative subpoenas, constitutionality "is predicated on the availability of a neutral tribunal to determine, after the subpoena is issued, whether a subpoena actually complies with the Fourth Amendment's demands."[51] An administrative subpoena regime would not be constitutional if judicial review was not available "prior to suffering penalties for refusing to comply."[52] In 2004, the Federal District Court for the Southern District of New York, in a decision upheld by the Court of Appeals for the Second Circuit, held that the statutory provision allowing the FBI to issue NSLs to internet service providers ("ISPs") but denying pre-enforcement review to the recipients was unconstitutional.[53] The ISPs argued that the non-disclosure provision effectively prevented them from accessing the courts because

47. 12 U.S.C.A. § 3414(b)(1) (West 2004) ("Nothing in this chapter shall prohibit a Government authority from obtaining financial records from a financial institution if the Government authority determines that delay in obtaining access to such records would create imminent danger.").

48. 18 U.S.C.A. § 3511(c) (West Supp. 2007); *see also* Brian T. Yeh & Charles Doyle, *USA Patriot Improvement & Reauthorization Act of 2005: A Legal Analysis* 14, CRS Report for Congress (Dec. 21, 2006), *available at* http://www.fas.org/sgp/crs/intel/RL3332.pdf.zx.

49. *See* 18 U.S.C.A. § 3511(c) (West Supp. 2007) (allowing the court to issue an order that requires a person to comply with the request).

50. *See* Doe v. Ashcroft, 334 F. Supp. 2d 471, 495 (S.D.N.Y. 2004), *vacated by* 449 F.3d 415 (2d Cir. 2006) (stating that an administrative subpoena derives justification from the judicial process).

51. *Id.* There are only a smattering of recent cases challenging NSLs, because "[w]ith no means to enforce or to quash NSLs and with NSLs being issued primarily to third parties with little reason to refuse compliance, challenges to the issuance of these administrative subpoenas only occurred after the publicity they garnered with the PATRIOT Act." Dinh, *supra* note 12, at xxix.

52. *Ashcroft*, 334 F. Supp. 2d at 495.

53. Doe v. Gonzales, 449 F.3d 415, 418 (2d Cir. 2006) (describing the ISP's argument that the original § 2709 was unconstitutional under the Fourth Amendment because it denied pre-enforcement review and under the First Amendment because "it operated as a content-based prior restraint on speech that was not sufficiently narrowly tailored to achieve a compelling governmental interest"); *see also* Doe v. Gonzales, 386 F. Supp. 2d 66, 83 (D. Conn. 2005) (granting a motion for a preliminary injunction enjoining the government from enforcing the gag order imposed on the recipient of an NSL under § 2709(c) because the recipient had demonstrated irreparable harm from the suppression of speech).

they would need to divulge the receipt of an NSL in order to litigate.[54] The court agreed, concluding that "what is, in practice, an implicit obligation of automatic compliance with NSLs violates the Fourth Amendment right to judicial access."[55] Courts have similarly rejected law enforcement processes compelling libraries to disclose borrower records without permitting pre-enforcement challenges.[56] As discussed above, the amended NSL provision in the Reauthorized Patriot Act allows recipients of the letters to challenge their issuance.[57] Because the Reauthorized Patriot Act added provisions explicitly permitting challenges and consultation with an attorney, the second circuit vacated the portion of the district court's holding that the NSL process was unconstitutional under the Fourth Amendment.[58]

While Congress was drafting the Patriot Act of 2001, the government originally sought administrative subpoena power but received only the authority to issue letters under section 215.[59] Although NSLs are like administrative subpoenas in that no judicial approval is required for authorization, they do not come with a self-executing enforcement mechanism.[60] Rather, if the recipient of the letter does not comply, the government must approach a federal court for enforcement.[61] This suggests that Congress intended the NSL process to confer only limited

54. *Ashcroft*, 334 F. Supp. 2d at 505.

55. *Id.* (reasoning that it would be naïve to think that "NSLs, given their commandeering warrant, do anything short of coercing all but the most fearless NSL recipient into immediate compliance and secrecy").

56. Doe v. Gonzales, No. 05A295 (Oct. 7, 2005) (denying emergency application), *available at* http://www.aclu.org/safefree/nationalsecurityletters/080306ginsburg_opinion_sealed .pdf (providing that requests for library records are unconstitutional for the same reasons as internet service provider records in *Doe v. Gonzales*, 449 F.3d 415, 419 (2d Cir. 2006)). *Compare* Jay M. Zitter, *Constitutionality of National Security Letters Issued Pursuant to 18 U.S.C.A. § 2709*, 2006 A.L.R. Fed. 2d, at 3 (noting that the NSLs held unconstitutional in the ISP and library contexts are different than those issued to financial institutions).

57. Doe v. Gonzales, 449 F.3d 415, 419 (2d Cir. 2006).

58. *Id*. (also vacating and remanding the First Amendment portion of *Doe v. Ashcroft* in response to the legislative changes).

59. COMM. ON THE JUDICIARY H.R. REP. NO. 107–236, pt. 1, at 61 (2001). *Compare* Endicott Johnson Corp. v. Perkins, 317 U.S. 501, 509 (1943) (providing that the court must enforce an administrative subpoena unless it is "plainly . . . irrelevant to any lawful purpose" of the agency).

60. Woods, *supra* note 16, at 61. Woods points out the distinction between 21 U.S.C. § 876(c), which provides for judicial enforcement of administrative subpoenas, and 12 U.S.C. § 3414(a)(5), which fails to provide for judicial enforcement of NSLs. *Id.* at n.150; *see also* Beryl A. Howell, *Surveillance Powers In The USA PATRIOT Act: How Scary Are They?*, 76 PA. B. ASS'N. Q. 12, 18 (2005) (explaining that outside of limited categories, the FBI must get a court order to obtain records).

61. *See* Doe v. Ashcroft, 334 F. Supp 2d 471, 485 (S.D.N.Y. 2004), *vacated by* 449 F.3d 415 (2d Cir. 2006) (explaining that like administrative subpoenas, when a recipient of an NSL refuses to comply, the agency who sent it can seek a court order for enforcement).

authority to government agencies and wished to give courts a role in balancing law enforcement power with personal liberties.

C. Non-Mandatory NSLs

As discussed in the previous Part, pre-enforcement approval by a judicial officer is not required for an agency to issue an NSL; rather, the agency director need only certify to the financial institution that the requested records are needed for foreign counterintelligence purposes. Several agencies order NSLs on a regular basis, namely the FBI, the CIA, and the DoD. However, only the FBI has been authorized by Congress to issue NSLs with which the recipient is required to comply. The CIA, DoD, and other agencies may issue NSLs, but because they lack express congressional authorization, compliance is voluntary and left to the discretion of the recipient.

In addition to the NSLs authorized by the Patriot Act, the U.S. military and the CIA have begun issuing "non-mandatory" NSLs as an extension of their domestic intelligence-gathering operations. The letters are mostly issued in connection with military or criminal investigations. The military and CIA lack explicit statutory authority to issue mandatory NSLs, and Congress has been reluctant to grant this power because of concerns that they should not be involved in domestic spying.[62] In addition, as Elizabeth Parker, a former general counsel at both the National Security Agency and the CIA, has observed, the letters contrast with the "strong tradition of not using our military for domestic law enforcement" and signify a "mov[e] into territory where historically they have not been authorized or presumed to be operating."[63] In general, courts have also reasoned that government surveillance in domestic affairs is entitled to greater constitutional protection than in the foreign intelligence context.[64] Despite their

62. Posting of Jonathan Winer to Counterterrorism Blog (Jan. 14, 2007), *available at* http://www.counterterrorismblog.org/2007/01/ [hereinafter Winer] ("Given that the FBI already had this authority and has been using it at the rate of some 9000 times per year, it is not clear why the CIA and Defense Department have needed it. The initial efforts to justify it raise more questions than they answer."). *But see* Lichtblau, *supra* note 41 ("Government lawyers say the legal authority for the Pentagon and the C.I.A. to use national security letters in gathering domestic records dates back nearly three decades and, by their reading, was strengthened by the antiterrorism law known as the USA Patriot Act.").

63. Lichtblau, *supra* note 41 (quoting Elizabeth Parker).

64. United States v. U.S. Dist. Court for E. Dist. Mich., S. Div., 407 U.S. 297, 316 (1972) ("Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch.").

questionable validity, officials estimate that thousands of these letters have been disseminated in the past few years.[65]

Although these requests are admittedly non-mandatory (in contrast to FISA requests or NSLs issued by the FBI), journalistic investigations have revealed that financial institutions typically produce documents voluntarily upon receiving NSLs.[66] For example, a noncompulsory NSL was used to solicit and obtain the financial records of a Muslim chaplain at Guantanamo Bay, a U.S. citizen who was falsely suspected of supporting terrorists.[67] Such disclosure raises serious civil liberties issues: "[W]hen the person under investigation is an American the justification for doing this without the normal procedural protections of a law enforcement investigation is hard to understand."[68]

The fact that the military and CIA are permitted to issue non-mandatory NSLs in a particular context does not mean that Congress would grant them the authority to issue a mandatory NSL under the same set of circumstances. Historically, Congress has limited the scope of the authority to issue mandatory NSLs. When Congress began to allow the FBI to issue mandatory NSLs, the Senate Intelligence Committee "concluded that the FBI's *mandatory* NSL power should be more limited in scope than what the FBI had been seeking under voluntary NSL arrangements."[69] Furthermore, although Congress has given the FBI the right to issue mandatory NSLs, this does not imply that Congress would willingly give the same authority to other federal agencies. Indeed, financial privacy statutes now prohibit the transfer of customer information across agencies, implying that Congress wishes to limit which agencies have access to particular forms of information.[70]

65. Lichtblau, *supra* note 41.

66. *Id*.

67. Karen DeYoung, *Officials: Pentagon Probed Finances*, WASH. POST., Jan. 14, 2007, at A12, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/01/13/AR2007011301486_pf.html; *see also* Laura Parker, *The Ordeal of Chaplain Yee*, USA TODAY, May 16, 2004, *available at* http://www.usatoday.com/news/nation/2004-05-16-yee-cover_x.htm (explaining that officials will not comment on why Yee was accused of espionage and that all criminal charges against Yee were eventually dropped).

68. Winer, *supra* note 62.

69. Doe v. Ashcroft, 334 F. Supp. 2d 471, 481 (S.D.N.Y. 2004), *vacated*, 449 F.3d 415 (2d Cir. 2006) (emphasis in original) (citing S. Rep. No. 99–307, at 19–20). The FBI was permitted to issue non-mandatory NSLs for any records "relevant to FBI counterintelligence activities." *Id.* However, the power to issue mandatory NSLs is limited to records pertaining to persons for whom there are "specific and articulable facts" indicating that the person is an agent of a foreign power. *Id*.

70. *E.g.*, Privacy Act of 1974, 5 U.S.C. § 552a(b) (2000); Peter P. Swire, *The Surprising Virtues of the New Financial Privacy Law*, 86 MINN. L. REV. 1263, 1275 (noting that the Privacy

III. PRIVACY RIGHTS OF DEPOSITORS IN INFORMATION CONVEYED TO FINANCIAL INSTITUTIONS

The Fourth Amendment protects individuals from unreasonable searches and seizures and explicitly mentions the right to be secure in one's "papers."[71] However, the Supreme Court has not interpreted the Fourth Amendment as protecting information voluntarily conveyed to a third party.[72]

To address this, Congress has passed several statutes heightening customer protections by restricting the circumstances under which banks can release financial information.[73] In 1978, Congress passed the Right to Financial Privacy Act ("RFPA") to protect bank customers from undue intrusion into their private records. In 1999, Congress enacted the Gramm-Leach-Bliley Act ("GLBA"), which tightened restrictions on the sharing of customer information and provided administrative oversight to curb unwarranted disclosures. These federal enactments and complementary state regimes enumerate express rights and obligations, which further thicken the historically rich set of duties that banks owe their customers.

Along with the federal and state legal regimes governing financial privacy, historic notions of privacy in financial information inform the reasonable expectations of customers, shaping their interpretations of institutional privacy policies and the perception of the bank-customer relationship.[74] Furthermore, banks explicitly take on certain duties by presenting their customers with privacy agreements guaranteeing that they will guard nonpublic information. Any discretion reserved by the bank in such agreements should be reviewed critically by courts because the contracts are standard forms drafted by the banks and lack bargained-for mutual intent.

Act has effectively "succeeded in preventing the creation of the omnivorous, unified federal database").

71. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, *papers*, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.") (emphasis added).

72. *E.g.*, United States v. Miller, 425 U.S. 435, 443 (1976) (stating that customers are not protected even if they convey information on the assumption that the third party will not convey it to others).

73. Right to Financial Privacy Act, 12 U.S.C. § 3401 (2000 & West Supp. 2002).

74. *See* Suburban Trust Co. v. Waller, 408 A.2d 758, 764 (Md. Ct. Spec. App. 1979) (holding that bank depositors should expect that their information will be kept private).

A. Limited Constitutional Protections of Financial Information

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[75] The bare language of the Fourth Amendment—particularly its inclusion of "papers"—might be construed as protecting bank depositors from disclosure of their financial information. However, the Supreme Court has interpreted the Fourth Amendment narrowly and afforded little privacy protection to bank customers in their books and records.[76]

In *Katz v. United States*, the Supreme Court declined to infer a general right to privacy from the Fourth Amendment, reasoning instead that the contours of privacy rights were generally to be determined by the individual states.[77] However, the Court found that the Fourth Amendment requires law enforcement agents to comply with the "procedure of antecedent justification" before engaging in searches and seizures.[78] In *Katz*, government agents electronically recorded the petitioner's calls made from a telephone booth.[79] The Court held that while the government agents exercised restraint in narrowly tailoring their surveillance, their actions were nonetheless improper because the agents failed to first obtain judicial authorization.[80] Essential to this outcome was the Court's recognition that the Fourth Amendment protected "people, not places" and hence applied to intangible as well as physical property.[81] In addition, the *Katz* Court focused on whether the individual had intended to make the information public rather than where the individual had chosen to store the information.[82] By doing so, *Katz* "underscored the crucial role that disclosed but nonpublic information plays in modern society."[83] The reasoning of the *Katz*

75. U.S. CONST. amend. IV.

76. *E.g.*, *Miller*, 425 U.S. at 443 (stating that the Fourth Amendment does not protect information voluntarily revealed to a third party).

77. Katz v. United States, 389 U.S. 347, 350–51 (1967).

78. *Id.* at 359.

79. *Id.* at 348.

80. *Id*. at 356–57 ("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 . . . .").

81. *Id*. at 351 ("But what [an individual] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

82. *Id.*; *see also* Andrew DeFillipis, Note, *Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence*, 115 YALE L.J. 1086, 1102 (2006) (*Katz* "began to articulate an affirmative right to control one's information by symbolic gestures and mutually recognized norms").

83. DeFillipis, *supra* note 82, at 1103.

decision left open the possibility that customer financial records might be protected under the Fourth Amendment.

However, in *United States v. Miller*, the Court closed this possibility by holding that the search and seizure of bank records does not violate the Fourth Amendment because "[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[84] The Court reasoned:

> "[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[85]

As a result, the Court held that the documents copied and seized by the government agents in the case were the bank's business papers and not the petitioner's private papers and hence did not merit Fourth Amendment protection.[86] In deciding not to grant constitutional protection to these records, the Court relied on its prior holding in *Hoffa v. United States* that the Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."[87]

Although the *Miller* decision effectively closed off constitutional avenues for seeking privacy protection for financial records, some lower courts have avoided the Supreme Court's holding by carving out privacy protections in analogous cases. For example, in a drug seizure case, the Sixth Circuit held that individuals retained a reasonable expectation of privacy in the contents of their safety deposit boxes even though the boxes ostensibly belonged to the bank.[88] However, when it comes to financial records per se, it appears that there is little

84. United States v. Miller, 425 U.S. 435, 443 (1976) (citing United States v. White, 401 U.S. 745, 751–52 (1971)). *But see* Stephen J. Schulhofer, *The New World of Foreign Intelligence Surveillance*, 17 STAN. L. & POL'Y REV. 531, 546 (2006) ("Even if a customer inevitably takes a risk that some companies and their employees might break such promises, the Supreme Court gave prosecutors something much broader: the power to compel the firm to turn over customer information when the firm seeks to honor its commitment to preserve confidentiality.").

85. *Miller*, 425 U.S. at 443–44 (citing *White*, 401 U.S. at 751–52). It should be noted, however, that financial records, as opposed to opinions about a customer's financial condition, are not protected under the First Amendment. *See, e.g.*, Schoneweis v. Dando, 435 N.W.2d 666, 671 (Neb. 1989) ("[D]eclarations that one's farm is in trouble and that one would lose everything are expressions of pure opinion protected by the First Amendment . . . .").

86. *Miller*, 425 U.S. at 443–44.

87. *Id.* at 443 (citing Hoffa v. United States, 385 U.S. 293, 302 (1966)).

88. United States v. Thomas, No. 88–6341, 1989 WL 72926, at *2 (6th Cir. Jul. 5, 1989).

constitutional ground on which to argue for the protection of customer privacy.[89]

In the alternative, some courts have reasoned that while customers do not retain Fourth Amendment rights in information they voluntarily convey to a bank, the bank itself may be entitled to this protection, either from its endogenous privacy interests or through transference from the customer. For example, in finding the earlier NSL process unconstitutional, the District Court for the Southern District of New York reasoned that "many potential NSL recipients may have particular interests in resisting an NSL, *e.g.*, because they have contractually obligated themselves to protect the anonymity of their subscribers."[90] Some state courts have also given weight to a bank's own interest in privacy. In Louisiana, one bank claimed that releasing private consumer financial information without customer consent would not only violate the Gramm-Leach-Bliley Act but also cause an irreparable injury to the bank, which feared that it would "surely suffer injury to its business reputation when its customers learn[ed] that their private financial information was divulged to third parties without their consent."[91] The state court agreed, stating, "Once this information has been provided, in contradiction to the dictates of the GLBA, there is no monetary relief which could compensate such a loss."[92] Hence, there may still be a few avenues available to require banks to challenge FISA requests or NSLs on purely constitutional grounds. However, this Article will not focus on solely constitutional ideals, as the rights of bank customers are strengthened by federal statutory protections passed in response to *Miller*.

B. Extensive Statutory Schemes

Although the Supreme Court did not recognize a constitutional right to privacy in one's bank records, Congress may extend individual privacy rights beyond this minimal constitutional guarantee.[93] Congress

89. *Cf.* Whalen v. Roe, 429 U.S. 589, 605 (1977) ("Recognizing that in some circumstances [the] duty [to avoid unwarranted disclosure of data] arguably has its roots in the Constitution . . . .").

90. Doe v. Ashcroft, 334 F. Supp. 2d 471, 494 n.118 (S.D.N.Y. 2004), *vacated*, 449 F.3d 415 (2d Cir. 2006).

91. Union Planters Bank v. Gavel, No. CIV.A.02–1224, 2002 WL 975675, at *2 (E.D. La. May 9, 2002).

92. *Id.* at *6; *see also* Cal. Bankers Ass'n v. Schultz, 416 U.S. 21, 51 (1974) ("It is true that in a limited class of cases this Court has permitted a party who suffered injury as a result of the operation of a law to assert his rights even though the sanction of the law was borne by another.").

93. H.R. REP. NO. 95–1383, at 28 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 9273, 9306.

is cognizant of its ability to expand privacy protections for personal information, noting in a House Committee Report: "[W]hile 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."[94] Congress has used its power to provide for some measure of individual control over information ceded to financial institutions through a series of legislative enactments over the decades since the *Miller* decision.[95] This Part will discuss the two statutory schemes most relevant to financial privacy in the context of law enforcement inquiries, the Right to Financial Privacy Act of 1978, and the Gramm-Leach-Bliley Act of 1998, along with state constitutional and statutory protections.[96]

1. The Right to Financial Privacy Act

In response to the rescission of financial privacy protection by the Supreme Court in *Miller*, Congress acted to explicitly endow bank customers with statutory protection for information exchanged in the course of financial transactions.[97] In 1978, Congress passed the Right to Financial Privacy Act ("RFPA"), which was "intended to protect the customers of financial institutions from unwarranted intrusion into their records while at the same time permitting legitimate law enforcement activity."[98] The accompanying house report specifically described the RFPA as an expansion of privacy protections in reaction to *Miller*, expressing concern that the decision "did not acknowledge the sensitive nature of [financial] records."[99] The RFPA prohibits financial institutions from disclosing records without notifying affected customers,[100] and requires customer consent absent a search warrant, judicial subpoena, or formal written request.[101] This enactment

94. *Id*.

95. Schulhofer, *supra* note 84, at 547 ("These state and federal statutes do not provide the full complement of Fourth Amendment safeguards . . . . Instead they establish a dense web of accountability provisions, with requirements and procedures that differ according to the kind of information concerned and the government's asserted purpose in seeking it.").

96. 12 U.S.C.A. § 3409 (West 2004 & Supp. 2007); 15 U.S.C. § 6801(a) (2000 & West Supp. 2002).

97. H.R. REP. NO. 95–1383, *supra* note 93, at 34.

98. H.R. Rep. No. 95–1383, *supra* note 93, at 34; Edward L. Symons, *The Bank-Customer Relation*, 100 BANKING L.J. 220, 237 (1983) ("In 1978, Congress expressed its determination that, contrary to the majority opinion in *Miller*, a bank customer has a reasonable expectation of privacy in his financial dealings with a bank.").

99. H.R. REP. NO. 95–1383, *supra* note 93, at 34.

100. 12 U.S.C.A. § 3409 (West 2004 & Supp. 2007).

101. 12 U.S.C. § 3404 (2000) (customer authorization); 12 U.S.C.A. § 3406 (search warrant); 12 U.S.C.A. § 3407 (subpoena); 12 U.S.C.A. § 3408 (written request). When the government

empowers customers to object when the bank is presented with an administrative summons or judicial subpoena by filing a motion to quash or applying to enjoin the soliciting government agency.[102] In addition, banks that violate the RFPA by failing to comply with its procedural safeguards may be subject to civil liability to the customer whose records were disclosed.[103]

However, the RFPA exempts from its procedural requirements investigations related to national security, counterterrorism, or foreign intelligence.[104] The protections above may be bypassed if the government authority certifies to the financial institution that "there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person."[105] Hence, the RFPA expanded customer protections in some areas but also remained deferential to the investigative powers of federal law enforcement agencies.

As originally enacted, the RFPA granted the FBI the authority to issue letters requesting records but did not require financial institutions to comply with the requests.[106] Rather, the RFPA tracked traditional law enforcement procedures that generally require that when the Government seeks financial records of bank customers as part of a law enforcement inquiry, it must use a formal written request such as a subpoena (that is reviewable in court) or obtain a search warrant.[107] In addition, the original RFPA required customer notice unless an order delaying notice was issued by a judicial officer.[108] These protections have eroded over time. The RFPA was amended in 1987 by the Intelligence Authorization Act "to grant the FBI authority to obtain a customer's or entity's records from a financial institution for counterintelligence purposes" in the face of "specific and articulable facts giving reasons to believe that the customer or entity is a foreign power or an agent of a foreign power."[109] Despite this change in the

subpoenas a customer's records, the government must also provide a copy of the subpoena to the customer and a notice specifying the nature of the inquiry, § 3407(2).

102. 12 U.S.C. § 3410(a) (2000) (discussing customer challenges).

103. 12 U.S.C. § 3417(a) (2000) (discussing civil penalties).

104. 12 U.S.C.A. § 3414(a)(1) (West 2004 & Supp. 2007).

105. 12 U.S.C.A. § 3414(a)(3)(A) (West Supp. 2007).

106. Right to Financial Privacy Act, 12 U.S.C.A. § 3414(a) (West Supp. 2007).

107. Robert T. Palmer & A.T. Darin Palmer, *Complying with the Right to Financial Privacy Act of 1978*, 96 BANKING L.J. 196, 211–12 (1979).

108. *Id.*

109. H.R. REP. NO. 99–690(I), at 14 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 5327, 5341.

evidentiary standard, the RFPA still reflects the importance of financial privacy as reaffirmed by Congress.

2. The Gramm-Leach-Bliley Act

On November 12, 1999, Congress passed the Gramm-Leach-Bliley Act ("GLBA") to modernize the regulation of financial institutions.[110] One component of this modernization was a reinvigoration of the central tenet of financial privacy. The GLBA reaffirmed the duty of financial institutions to guard the privacy of their customers' information.[111] Like the RFPA, the GLBA requires financial institutions to notify customers whose records have been solicited and to provide an opportunity for affected customers to opt out of the disclosure.[112] However, it also contains a judicial process exception, allowing the financial institution to disclose personal information as necessary to comply with a subpoena, summons, other judicial process, or as authorized by law.[113] Unlike the RFPA, the GLBA is focused on administrative oversight rather than the enforcement of private rights.[114] Although the GLBA does not grant any new rights to depositors in the face of law enforcement inquiries, its legislative history demonstrates Congress' intent to preserve and strengthen the relationship between financial institutions and their customers. Industry groups opposed the GLBA's tightened restrictions on the sharing of customer information.[115] However, Congress was persuaded by testimony that customers consider the information they reveal to financial institutions to be private. The Honorable Edward Gramlich, a member of the Board of Governors of the Federal Reserve, testified that:

---

110. Gramm-Leach-Bliley Act (also known as the Financial Services Modernization Act of 1999), Pub. L. No. 106–102, 113 Stat. 1338 (Nov. 12, 1999) (codified as 15 U.S.C.A. § 6801 (West 2004)).

111. 15 U.S.C. § 6801(a) (2000 & West Supp. 2007).

112. The Gramm-Leach-Bliley Act: The Financial Privacy Rule, 16 C.F.R. pt. 313 (2000), *available at* http://www.ftc.gov/os/2000/05/65fr33645.pdf.

113. 15 U.S.C. § 6802(e)(8) (2000 & West Supp. 2007); *see, e.g.*, *Ex parte* Mutual Savings Co., 899 So. 2d 986, 992–93 (Ala. 2004) (holding that the trial court could order disclosure of customer information during civil discovery as part of GLBA's judicial-process exception).

114. David W. Roderer, *Tentative Steps Toward Financial Privacy*, 4 N.C. BANKING INST. 209, 212–13 (2000) ("[T]he new federal law does not empower consumers to act to ensure their own interests in such matters. Rather, the law establishes a procedural device and overlapping regulatory supervisory enforcement mechanisms to identify and correct abusive policies and practices rather than to remedy or resolve individual rights affected by specific infractions."); *see also* 15 U.S.C. § 6801 (West 2004) (requiring agencies to "establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards to insure the security and confidentiality of customer records and . . . to protect against unauthorized access to or use of such records").

115. Roderer, *supra* note 114, at 215.

> Control of information about ourselves is a fundamental means by which we manage our relationships with each other. The feeling that financial information should be private has deep historic roots, and bankers and customers have long viewed their business relationship as involving a high degree of trust which could be threatened by violation of privacy.[116]

Furthermore, Mr. Gramlich considered whether banking practices governing the treatment of customer information were evolving too quickly for customers or market forces to adjust to them.[117] In light of these rapid changes and lagging responses, he urged Congress to "strike the appropriate balance between these competing interests."[118] Congress responded with the GLBA, which improved the ability of customers to exercise control over the dissemination of information contained in their bank records.

3. State Constitutional and Statutory Protections

Even when interpreting the Fourth Amendment narrowly with regard to financial privacy, the Supreme Court has cautioned: "Our holding, of course, does not affect the State's power to impose higher standards on searches and seizures than required by the Federal Constitution if it chooses to do so."[119] State courts in a multitude of jurisdictions have accepted this as an open invitation to distinguish the applicability of *Miller* when they encounter more protective state regimes.[120] For example, the Colorado Supreme Court noted that while it was bound by the Supreme Court's interpretation of the Fourth Amendment, *Miller* did not constrict state constitutional protections.[121]

---

116. *Financial Privacy: Hearing on H.R. 10 Before the Subcomm. on Financial Institutions and Consumer Credit of the Comm. on Banking and Financial Servs.*, 106th Cong. 129 (1999) (statement of Edward Gramlich, Member, Board of Governors, The Federal Reserve System), *available at* http://commdocs.house.gov/committees/bank/hba58308.000/hba58308_1.HTM [hereinafter Gramlich Statement]. *See generally* Indiv. Reference Servs. Group, Inc. v. FTC, 145 F. Supp. 2d 6, 18–20 (D.D.C. 2001) (providing an extensive discussion of legislative history of the GLBA).

117. Gramlich Statement, *supra* note 116.

118. *Id.*

119. Cooper v. California, 386 U.S. 58, 62 (1967).

120. *See* People v. Jackson, 452 N.E.2d 85, 88 (Ill. App. Ct. 1983) ("A State may of course set a higher standard of rights than the comparable United States constitutional right . . . . Colorado, California and Pennsylvania rejected the rationale of *Miller* and held that there was a privacy right in bank records and consequently there was standing."); *see also* Commonwealth v. Harris, 239 A.2d 290, 292 n.2 (Pa. 1968) ("[T]he state has the power to impose standards on searches and seizures higher than those required by the Federal Constitution.").

121. Charnes v. DiGiacomo, 612 P.2d 1117, 1120 (Colo. 1980); *see also* Jerome B. Falk, *The State Constitution: A More Than "Adequate" Nonfederal Ground*, 61 CAL. L. REV. 273, 283–84 (1973) ("For a state court interpreting a state constituion [sic], opinions of the United States

Many state courts have analyzed the right to privacy in bank records under *Katz* instead of *Miller*.[122] In doing so, some have explicitly declined to follow *Miller* out of a belief that it "establishes a dangerous precedent, with great potential for abuse."[123] For example, the Colorado courts, following the lead of the California courts, applied the "*Katz* expectation of privacy test as a measure of unreasonable seizures under the Colorado Constitution" in determining whether a customer had the right to challenge a subpoena to the bank for his records.[124] In an analogous move, the Illinois state courts reasoned that since *Katz* held that an individual's reasonable expectation of privacy in personal papers is not contingent on his or her location, "the right to privacy is not waived by placing these records in the hands of a bank."[125]

However, state constitutional protections of privacy in financial records are typically not absolute and the conferred rights are balanced against competing policy concerns. In upholding a subpoena that prevented notice to the customer whose records were solicited, a Florida state court noted that the bank customers' right of privacy in bank records was a state constitutional right that yielded to an investigation of the pari-mutuel industry, which, to be effective, was to be conducted without notice.[126] However, the court recognized the case as an exception to the general state constitutional protection of financial privacy.[127]

Along with constitutional provisions, many states have enacted statutory schemes that provide more robust and particularized protection of financial privacy rights. For example, Louisiana has enacted a statutory scheme which its state courts have interpreted as imbuing

---

Supreme Court are like opinions of sister state courts or lower federal courts. . . . [A] difference in reasoning should be no more alarming than the differences which impel one judge to dissent from another's opinion . . . ."); William J. Brennan, Jr., *State Constitutions & the Protection of Individual Rights*, 90 HARV. L. REV. 489, 491 (1977) ("[S]tate courts cannot rest when they have afforded their citizens the full protections of the federal Constitution. State constitutions, too, are a font of individual liberties, their protections often extending beyond those required by the Supreme Court's interpretation of federal law.").

122. *E.g.*, State v. Thompson, 810 P.2d 415, 417–18 (Utah 1991) ("Several state courts have rejected the rationale of *Miller* and have held that under their state constitutions, a bank customer has a privacy right in bank records . . . . These courts have found the rationale in *Katz* . . . to be more persuasive than that of *Miller*.").

123. Commonwealth v. DeJohn, 403 A.2d 1283, 1289 (Pa. 1979).

124. *Charnes*, 612 P.2d at 1120; Burrows v. Superior Court, 529 P.2d 590, 592–93 (Cal. 1974) (relying on Art. I, sec. 13 of the California Constitution).

125. People v. Jackson, 452 N.E.2d 85, 88 (Ill. App. Ct. 1983) (citing *Burrows*, 529 P.2d at 593–95).

126. Winfield v. Div. of Pari-Mutuel Wagering, 477 So.2d 544, 547–48 (Fla. 1985).

127. *Id.*

banks with a duty of confidentiality.[128] Banks have statutory authority to disclose customer records when faced with a subpoena, summons, or court order, but even for these formal inquiries, the affected customer must be notified when permitted and given an opportunity to object in a timely manner.[129] The courts have interpreted this customer protection broadly: "Thus, although neither statute specifically contains any language which expressly creates a cause of action in favor of an individual whose records were wrongfully disclosed, we find that these statutes create a duty of confidentiality on the part of financial institutions in favor of their customers."[130]

Maryland has a more explicit state regime protecting the rights of bank customers.[131] The Maryland legislature was "[a]pparently disturbed by what it believed to be the trend, out of all scotch and notch, among banks and other fiduciary institutions to furnish information without compulsion to government agencies"[132] and sought to re-emphasize the importance of confidentiality in bank-customer dealings.[133] In light of its statutory regime, Maryland state courts have interpreted the circumstances under which these customer confidences can be breached very narrowly, limiting banks to disclosing customer information only under lawful court order or with customer consent, holding that[134] "absent compulsion by law, a bank may not make any disclosures concerning a depositor's account without the express or implied consent of the depositor."[135]

128. Confidential Nature of Financial Information and Financial Records, LA. REV. STAT. ANN. § 40:2106 (2000).

129. Burford v. First Nat'l. Bank in Mansfield, 557 So.2d 1147, 1150–51 (La. Ct. App. 1990).

130. *Id.* at 1151.

131. MD. CODE ANN., Financial Institutions § 1–306(b) (LexisNexis 2003).

132. Suburban Trust Co. v. Waller, 408 A.2d 758, 764 (Md. Ct. Spec. App. 1979).

133. Preamble to Chapter 252(a)(2), 1976 Md. Laws 762–63.

134. *Suburban*, 408 A.2d at 765 (distinguishing the lower court's jury instruction, which told jurors that banks may release confidential information when "a matter of public necessity," reasoning that it "afforded the Bank more protection than it was entitled to receive"). The robustness of the rights created by these state statutory schemes is most evident by a comparison to states lacking such enactments. For example, the Indiana state courts have rejected the holding of *Suburban* because Indiana lacks a comparable statutory scheme. In the absence of rights creating statutory language, the Indiana courts have held that "a person does not legitimately expect his affairs with third parties to be kept private from law enforcement officers conducting an investigation." Ind. Nat'l Bank v. Chapman, 482 N.E.2d 474, 482 (Ind. App. 1985) (citing *In re* Order for Ind. Bell Tel, 409 N.E.2d 1089, 1090 (Ind. 1980)) ("[B]ank depositors have taken the risk in revealing their affairs to third parties that the information will be conveyed by that person to law enforcement officials, either voluntarily or in response to compulsory process."). Indiana courts have also held that public duty is sufficient to justify disclosure, even in the absence of formal process or compulsion by law. *Id.* at 482 n.4.

135. *Suburban*, 408 A.2d at 764.

New Hampshire has a similarly restrictive state statutory scheme, permitting the inspection of financial records by law enforcement officials only under a judicial subpoena or summons that describes the requested records with sufficient particularity.[136] These requirements go beyond "minimum constitutional requirements for the issuance of a search warrant."[137] When the state statutory requirements are not met, bank customers have standing to challenge any evidence obtained without procedural authorization.[138] Alabama has also enacted statutes which prohibit the disclosure of customer bank records except upon subpoena or court order.[139] These state enactments not only provide additional safeguards and courses of action for bank customers but also underscore the importance of financial privacy in society's collective consciousness.

C. Contractual Obligations of Banks

The express statutory sources of federal and state privacy rights discussed above are only a recent addition to the unique relationships banks and customers have developed with complex allocations of responsibilities and obligations. In a departure from the simple paradigm of a bare debtor-creditor relationship, banks have assumed roles as agents and fiduciaries, hence implicating the duties of confidentiality and loyalty.

Many banks have characterized the bank-customer relationship as more than just that of creditor and debtor. Rather, varying levels of loyalty and agency have been imputed to banks given the private nature of financial information. Furthermore, courts have considered the circumstances surrounding the formation of the bank-customer relationship in determining that banks entered into implied contracts with their customers and inferring an implied provision of confidentiality. Finally, courts have also held banks to their own guarantees of nondisclosure.

136. Obtaining Records by Search Warrant, N.H. REV. STAT. ANN. § 359–C:9 (LexisNexis 1995 & Supp. 2006); N.H. REV. STAT. ANN. § 359–C:4(I)(c) (LexisNexis 1995 & Supp. 2006).

137. State v. Sheedy, 474 A.2d 1042, 1044 (N.H. 1984).

138. *See id.* at 1044–045 (granting motion to suppress evidence obtained outside statutory requirements); State v. Flynn, 464 A.2d 268, 274 (N.H. 1983) (discussing right to challenge evidence gleaned from privacy violation).

139. Comment to Disclosure of customer financial records, ALA. CODE § 5–5A–43 cmt. (LexisNexis 1996 & Supp. 2006).

1. Implied Duty of Confidentiality

a. Duty of Confidentiality in the Bank-Customer Relationship

Under a classic debtor-creditor relationship, there is no expectation of privacy.[140] However, courts have hesitated to classify the bank and customer as merely a debtor and creditor.[141] Rather, judicial descriptions of the relationship operating within the broadly construed confines of the debtor-creditor model have heightened the classic conception by inferring a limited duty of privacy: "[T]he relationship between a general depositor and his bank is that of creditor-debtor, not a fiduciary relation, but the relation may give rise to some particular obligation, such as an obligation upon the bank not to disclose matters pertaining to the customer's account without his consent."[142] Some courts have harmonized the creditor-debtor and privity aspects of the bank-customer relationship by distinguishing between the duty of the bank with regard to the customer's money and to the customer's records.[143] One reason for this distinction between deposited money and bank records is the high value placed on financial privacy.[144] As courts in several jurisdictions have recognized: "Of all the rights of the citizen, few are of greater importance . . . [than] exemption of his private affairs, books, and papers from the inspection and scrutiny of others."[145]

While some courts have imputed an additional layer of confidentiality by supplementing the debtor-creditor paradigm, other courts have relied on a principal-agent model to deduce a duty of confidentiality. For example, the Idaho state courts have held that "in discharging its obligation to a depositor a bank must do so subject to the

140. Schoneweis v. Dando, 435 N.W.2d 666, 673 (Neb. 1989). However, the *Schoneweis* court distinguishes between the bank's duty to depositors and borrowers, finding no such duty of privacy with regard to the latter.

141. *E.g.*, Frame v. Boatman's Bank, 824 S.W.2d 491, 495 (Mo. Ct. App. 1992); Brex v. Smith, 146 A. 34, 36 (N.J. Ch. 1929) (finding additional duties implicit in the relationship between a bank and its customers).

142. *Frame*, 824 S.W.2d at 495 (citing Pigg v. Robertson, 549 S.W.2d 597, 600 (Mo. Ct. App. 1977)).

143. *Brex*, 146 A. at 36 ("It may be that the relation of a bank to its depositors is that of debtor and creditor, but I think it is more than that. As far as the money actually deposited is concerned, that is true. But, as to the records . . . [t]here is an implied obligation . . . on the bank, to keep these from scrutiny until compelled by a court of competent jurisdiction to do otherwise.").

144. *See In re* Pacific Ry. Comm'n, 32 F. 241, 251 (C.C.N.D. Cal. 1887) (describing compulsory production of private material without judicial process as "contrary to the principles of a free government").

145. *Id.* at 250; *see also* Interstate Commerce Comm'n v. Brimson, 154 U.S. 447, 479–80 (1894) (discussing demands for the production of documents such as bank records).

rules of agency."[146] In so finding, the court cited a variety of cases across jurisdictions holding that banks must comply with their depositors' orders.[147] Relying on cases where courts have held banks liable as agents of their customers with regard to forged checks, the *Peterson* court stated that the bank acted as its customers' agent for the purpose of disclosing information.[148] From this characterization the court inferred that the duty of confidentiality that prohibits an agent from disclosing information to the principal's detriment applies with regard to banks disclosing customer information.[149] The court stated: "[A]n agent is subject to a duty to the principal not to use or to communicate information confidentially given him by the principal or acquired by him . . . ."[150] Even if a bank cannot be considered a pure agent of its customers, its role and behavior may give rise to the expectation that it will accord with the principles of agency in controlling the dissemination of customer information.

Although courts impute notions of confidentiality and agency into the bank-customer relationship, they stop short of classifying banks as the fiduciaries of depositors absent special circumstances.[151] In a fiduciary

146. Peterson v. Idaho First Nat'l Bank, 367 P.2d 284, 288-89 (Idaho 1961).

147. *See, e.g.*, Dalamatinsko v. First Union Trust & Sav. Bank, 268 Ill. App. 314 (1932); Crawford v. W. Side Bank, 2 N.E. 881, 881 (N.Y. 1885) ("[I]n discharging its obligation as a debtor the bank must do so subject to the rules obtaining between principal and agent."). Courts have also recognized that agency also entails loyalty in executing the principal's orders. Finding that the relationship of the bank to its customers "was not only that of debtor and creditor but also that of agent and principal," the court concluded that "[t]he bank owed them the duty of loyalty which every agent owes its principal." Third Nat'l Bank v. Carver, 218 S.W.2d 66, 70 (Tenn. Ct. App. 1948) (holding that the bank breached its duty in paying a check despite depositor's stop order). However, agency may not govern all banking transactions. As the Nebraska courts have distinguished: "A debtor-creditor relationship exists with respect to funds on deposit and a principal-agent relationship exists with respect to the payment by the bank of checks drawn by a depositor." Selig v. Wunderlich Contracting Co., 69 N.W.2d 861, 866 (Neb. 1955) (citing 9 C.J.S. *Banks & Banking* § 267).

148. *Peterson*, 367 P.2d at 288.

149. Philip Blumstein & Linda A. Pohly, *Confidentiality, Access & Certainty: Disclosure of Customer Bank Records*, 1 ANN. REV. BANKING L. 101, 114 (1982).

150. *Peterson*, 367 P.2d at 289 (quoting RESTATEMENT (SECOND) OF AGENCY § 395 (1958)).

151. "[T]he relationship of the institution to the depositor is not typically deemed to be fiduciary in nature. Thus . . . absent special circumstances taking it out of the general rule, there is no aspect of a trust in the transaction." 10 AM. JUR. 2D *Banks & Fin. Inst.* § 720 (1997). In cases where customers allege that they have a fiduciary relationship with the bank, they are typically claiming that the bank had a *duty of disclosure* to the customer regarding another customer's financial condition, as opposed to a duty of confidentiality. *See, e.g.*, Hooper v. Barnett Bank of W. Fla., 474 So. 2d 1253, 1259 (Fla. Dist. Ct. App. 1985) ("[W]here a fiduciary duty to disclose may arise under the facts and circumstances, the jury is entitled to weigh this duty to disclose against the bank's duty of confidentiality . . . ."). *But see, e.g.*, United States v. First Nat'l Bank of Mobile, 67 F. Supp. 616, 624 (S.D. Ala. 1946) (considering banks to be the fiduciaries of their depositors).

relationship, the fiduciary has a duty to act primarily for the benefit of another.[152] Banks are not generally considered fiduciaries because "[i]t is typically not expected that the bank will exercise its powers primarily for the benefit of the customer. Rather, it is more commonly the expectation that the bank may exercise its power over property deposited for its own benefit."[153] Although fiduciary relationships are creatures of contract and malleably turn on the reasonable expectations of the parties, most courts and scholars agree that the typical conduct of banks and their customers does not create a reasonable expectation of a fiduciary relationship.[154] Although banking transactions do not create fiduciary duties by default, fiduciary relationships are not foreign to the banking industry and may arise under particular circumstances such as "a business or confidential relationship which induces one party to relax the care and vigilance it would ordinarily have exercised in dealing with a stranger."[155] Under such circumstances, financial institutions may be liable for disclosing customer information in breach of the duty of confidentiality.[156] In addition, a fiduciary relationship can arise from a "relationship of [] trust[] or superior knowledge . . . ."[157] For example, a bank may have a fiduciary relationship to its customer when acting as a financial advisor rather than merely as a depository institution.[158]

Although customers do not benefit from the full protections of a fiduciary relationship, the concept of agency along with the special value placed on financial records imputes some privacy protections into the bank-customer relationship. Some courts recognize that a bank implicitly agrees to hold customer information in confidence.[159] In

152. RESTATEMENT (SECOND) OF TRUSTS §§ 2, 170 cmt. a (1959).

153. Symons, *supra* note 98, at 232.

154. *Id.* at 231 (citing RESTATEMENT (SECOND) OF AGENCY §§ 1 cmt. b, 15 (1958)) (explaining that the bank-customer relationship cannot be considered truly fiduciary because banks may personally profit from the money deposited by customers).

155. Edward J. Raymond, Jr., Annotation, *Bank's Liability, Under State Law, for Disclosing Financial Information Concerning Depositor or Customer*, 81 A.L.R. 377, 390 § 7 (1990).

156. *Id.* (discussing Rubenstein v. South Denver Nat'l Bank, 762 P.2d 755 (Colo. Ct. App. 1988)).

157. Broadway Nat'l Bank v. Barton-Russell Corp., 585 N.Y.S.2d 933, 945 (N.Y. Sup. Ct. 1992).

158. *See* Gaunt v. Peoples Trust Bank, 379 N.E.2d 495, 496 (Ind. Ct. App. 1978) (recognizing a duty to act as more than a depositor in unspecified instances); Klein v. First Edina Nat'l Bank, 196 N.W.2d 619, 623 (Minn. 1972) (finding a duty to disclose to counsel only when special circumstances exist).

159. Suburban Trust Co. v. Waller, 408 A.2d 758, 764 (Md. Ct. Spec. App. 1979) (holding that absent legal compulsion, the bank could not reveal bank account information to police); White v. Regions Bank, 729 So.2d 856 (Ala. Civ. App. 1998). Although Maryland has a protective statutory scheme governing bank records, much of the *Suburban* court's reasoning was based on generally applicable historical and contextual reasoning.

addition, even when the level of dependence and trust placed in the bank by the customer does not emulate a fiduciary model, courts have noted that "intimate, private information is not furnished to any bank official lightly, nor, strictly speaking, voluntarily. . . . The delicately balanced relationship thus temporarily created is not . . . one composed of equals because of the inordinate power of the bank."[160] Courts have imputed a duty of confidentiality on banks to counterbalance the asymmetrical relationship of the vulnerable borrower and the institutional lender.[161] Hence, while banks are not the fiduciaries of their depositors, they do not enjoy unbridled discretion with regard to customer records.

b. Duty of Confidentiality Implied in Contract

Courts have recognized implied contracts where the elements of a contract can be inferred from the conduct of the parties, even in the absence of a written instrument.[162] Unlike cases where there is no express contract and the entire agreement must be implied, bank-customer arrangements are usually formalized through written contracts. However, the "relations of and the communications between the parties" may impute additional duties or obligations into the contract.[163] As Edward Gramlich testified to Congress: "In the area of financial information, many customers clearly believe that an implicit contract exists between the financial institution and the customer requiring the financial institution to keep information confidential."[164]

Courts have historically found confidentiality to be an implied term in bank-customer agreements. In 1924, the King's Bench in England reasoned that when interpreting a contract: "The Court will only imply terms which must necessarily have been in the contemplation of the parties in making the contract. . . . I have no doubt that it is an implied

160. Djowharzadeh v. City Nat'l Bank, 646 P.2d 616, 619 (Okla. Civ. App. 1982).

161. *Id.* at 619–20.

162. Marshall Contractors, Inc. v. Brown Univ., 692 A.2d 665, 669 (R.I. 1997); *see also* Hercules, Inc. v. United States, 516 U.S. 417, 424 (1996) ("[A]greement implied in fact is 'founded upon a meeting of minds, which, although not embodied in an express contract, is inferred, as a fact, from conduct of the parties showing, in the light of the surrounding circumstances, their tacit understanding.'") (citing Balt. & Ohio R.R. Co. v. United States, 261 U.S. 592, 597 (1923)).

163. *Marshall Contractors*, 692 A.2d at 669; *see also* U.C.C. § 1–205(3) (2004) ("A course of dealing between parties and any usage of trade in the vocation or trade in which they are engaged or of which they are or should be aware give particular meaning to and supplement or qualify terms of an agreement.").

164. *See* Gramlich Statement, *supra* note 116 (discussing the importance of controlling financial information to keep it private).

term of a banker's contract with his customer that the banker shall not disclose the account . . . ."[165] This notion was adopted by American banking law, which came to recognize confidentiality as a duty implied in the contract.[166] As federal courts have recognized: "All agree that a bank should protect [its] business records from the prying eyes of the public, moved by curiosity or malice. No one questions its right to protect its fiduciary relationship with its customers, which, in sound banking practice, as a matter of common knowledge, is done everywhere."[167]

Courts in the United States have applied this same line of reasoning in determining that bank customers maintain a reasonable expectation of privacy in their dealings. For example, one state supreme court reasoned that it is implied from the bank-customer relationship that banks should not disclose customer information without authorization, and that any unauthorized disclosures could make the bank subject to liability for breach of implied contract.[168] Giving determinative weight to implied duties of confidentiality, courts have held banks liable for breach of contract even when the bank's behavior did not violate any state or federal privacy statutes.[169]

165. Tournier v. Nat'l Provincial & Union Bank, 1 K.B. 461, 480 (1924) ("It is an implied term of the contract between a banker and his customer that the banker will not divulge to third persons, without the consent of the customer express or implied . . . unless the banker is compelled to do so by order of a Court . . . ."); *see also* 10 AM. JUR. 2D *Banks & Fin. Inst.* § 332 (1997) (discussing banking privacy issues).

166. ZOLLMANN'S BANKS & BANKING § 3413 (Kennth K. Luce ed., Supp. 1954) ("Depositors have a right of secrecy. A bank therefore is under an implied obligation to keep secret its records of accounts, deposits, and withdrawals."); IAN F.G. BAXTER, THE LAW OF BANKING AND THE CANADIAN BANK ACT 21–22 (2d ed. 1968) (discussing four exceptions to the duty of secrecy: "(a) disclosure under compulsion of law, (b) where there is a duty to the public to disclose, (c) where the interests of the bank require disclosure, (d) where the disclosure is made with the express or implied consent of the customer"). However, subsequent courts have recognized only exceptions (a) and (d). *E.g.*, Peterson v. Idaho First Nat'l Bank, 367 P.2d 284, 289 (Idaho 1961); Suburban Trust Co. v. Waller, 408 A.2d 758, 764 (Md. Ct. Spec. App. 1979); Brex v. Smith, 146 A. 34, 36 (N.J. 1929) (listing cases which have recognized the aforementioned exceptions).

167. United States v. First Nat'l Bank, 67 F. Supp. 616, 624 (S.D. Ala. 1946); *see also* THE PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 346 (U.S. Gov't Printing Office 1977), *available at* http://aspe.hhs.gov/datacncl/1977privacy/c9.htm ("The balance to be struck 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.").

168. Peterson v. Idaho First Nat'l Bank, 367 P.2d 284, 290 (Idaho 1961).

169. Taylor v. NationsBank, 776 A.2d 645, 653, 656–57 (Md. 2001) (holding that a bank which released its customer's records without consent or compulsion was liable for breach of contract, privacy, and confidentiality but finding no statutory violations).

Furthermore, the behavior of banks encourages customers to believe that they are entering into a confidential relationship. Noting that the existence of a confidential relationship requires both that the customer trust the bank to hold his information as confidential and that the bank invite or accept this trust, courts have stated that "banks present a constant invitation to intending borrowers, and thus subject themselves to whatever implication or obligation is to be drawn from that fact."[170] For example, as Bryant Bank promises in its Privacy Statement: "At Bryant Bank, it is trust that is the basis for each customer relationship. . . . We believe that your privacy should not be compromised."[171] Similarly, First Guaranty Bank states, "A fundamental component of any relationship is trust that the bank will respect the privacy and confidentiality of that relationship. First Guaranty Bank understands and realizes that we have a special duty to our customers to safeguard and protect your sensitive information."[172] In light of these expansive proclamations of financial privacy, Congress and various state legislatures have enacted legislation to enumerate some of the common expectations of bank customers.[173] Hence, most courts agree that at a minimum, "a bank has an obligation to its customers not to disclose unnecessarily, promiscuously, or maliciously their financial condition."[174] The Supreme Court has looked to the banking tradition of confidentiality in holding that the reasonableness of a privacy expectation depends upon current societal norms and upon the context in which the expectation arose.[175]

Courts are typically sympathetic to customers whose records have been disclosed without their consent because they do not consider information revealed to banks by customers as "entirely volitional, since it is impossible to participate in the economic life of contemporary

170. M.L. Stewart & Co. v. Marcus, 207 N.Y.S. 685, 692 (1924); Dolton v. Capitol Fed. Sav. & Loan Ass'n, 642 P.2d 21, 24 (Colo. Ct. App. 1981).

171. Bryant Bank, Privacy Statement (2005), http://www.bryantbank.com/index.asp?page =951 (last visited Aug. 24, 2007).

172. First Guaranty Bank, Privacy Policy (2006), http://www.fgb.net/PrivacyPolicy.htm (last visited Aug. 24, 2007).

173. Symons, *supra* 98, at 245 ("These expectations or perceived needs have arisen either from implicit or explicit assurances through advertising and other inducements toward an attitude of trust, or from a perceived community standard of what is right.").

174. Rubenstein v. S. Denver Nat'l Bank, 762 P.2d 755, 756 (Colo. Ct. App. 1988) (citing State v. McCray, 551 P.2d 1376, 1380 (Wash. Ct. App. 1976)).

175. O'Connor v. Ortega, 480 U.S. 709, 715–17 (1987) (discussing whether an employer's search of an employee's workplace is considered a violation of the employee's Fourth Amendment rights).

society without maintaining a bank account."[176] Even the American Banking Association has espoused the position that, "A bank should, as a general policy, consider information concerning its customers as confidential, which it should not disclose to others without clear justification."[177] Financial records are particularly sensitive because "the totality of bank records provides a virtual current biography."[178] When providing such extensive information to banks, customers expect that the information will only be used internally.[179] This view has been embraced by many jurisdictions. For example, the Supreme Court of Utah reasoned:

> [U]nder an expectation of privacy test, it is reasonable for our citizens to expect that their bank records will be protected from disclosure because in the course of bank dealings, a depositor reveals many aspects of her personal affairs, opinion, habit and associations which provide a current biography of her activities. . . . Since it is virtually impossible to participate in the economic life of contemporary society without maintaining an account with a bank, opening a bank account is not entirely volitional and should not be seen as conduct which constitutes a waiver of an expectation of privacy.[180]

Similarly, the Supreme Court of Pennsylvania held that borrowers and depositors have a "right to be free from unreasonable searches and seizures" of papers and other information supplied to banks during the transaction of financial business under a reasonable expectation of confidentiality.[181]

2. Explicit Duties of Confidentiality Created by Contractual Language

Banks and customers may buttress these background notions of confidentiality by contract. Indeed, some commentators have noted that instead of pigeonholing relationships into dichotomous categories such

176. Burrows v. Super. Ct. of San Bernardino Valley, 529 P.2d 590, 596 (Cal. 1974); *see also* Schulhofer, *supra* note 84, at 546 ("Indeed, the Court's approach paradoxically allows self-protection by actual criminals (who of course can choose to conduct their illegal transactions in cash) while leaving the law-abiding citizen with no practical way to shield the privacy of her daily life.").

177. *Compare* Milohnich v. First Nat'l Bank of Miami Springs, 224 So. 2d 759, 761 (Fla. Dist. Ct. App. 1969) (finding a breach of implied contractual duty for disclosure to third parties) *with* 12 C.F.R. § 309.1 (2007) (disclosure of information guidelines for the Federal Deposit Insurance Corporation).

178. *Burrows*, 529 P.2d at 596.

179. *See* Blumstein & Pohly, *supra* note 149, at 109–10 (describing the *Burrows* opinion).

180. State v. Thompson, 810 P.2d 415, 418 (Utah 1991) ("Such a biography should not be subject to an unreasonable seizure by the State government.") (quoting People v. Jackson, 452 N.E.2d 85, 89 (Ill. App. Ct. 1983)).

181. Commonwealth v. DeJohn, 403 A.2d 1283, 1291 (Pa. 1979).

as debtor-creditor or fiduciary, courts should analyze the bank-customer relation under a contractual model.[182] Such deference to contracts would not only better reflect the parties' intent but also encourage more precise contracting.[183]

Banks currently present customers with privacy agreements that speak to customer confidentiality in sweeping and deferential terms:

> We recognize the customer[s'] right to privacy and consider the confidentiality and safekeeping of customer information to be one of our fundamental responsibilities. And while information is critical to providing quality service, we recognize that one of our most important assets is our customers[s'] trust, therefore, confidentiality and safekeeping of customer information is a priority.[184]

Such customer agreements invoke notions of privacy that closely track the conception of confidentiality espoused in *Brex*,[185] *Burrows*,[186] *Suburban*,[187] and *Peterson*,[188] and shape the expectations of customers. Although banks voluntarily adopt these privacy policies, the promises of confidentiality and nondisclosure become part of the customer's expectations, thereby creating enforceable contractual rights.[189] These privacy agreements also represent a change in expectations of privacy since *Miller* was decided thirty years ago. Banks now advertise their privacy policies and typically allow customers to express preferences about how their non-public information can be used. As a result, customers today have a reasonable expectation that banks will not disclose their personal financial information.[190]

182. Symons, *supra* note 98, at 221–22 (noting that labels such as agent or fiduciary are "nothing more than specialty contract relations—contract relations shaped by recurring special facts and circumstances").

183. *Id.* (arguing that giving greater weight to contractual obligations "may encourage banks both to provide customers with a written elaboration of the true agreement and to take the time to be reasonably certain that the important aspects of the true agreement are effectively communicated . . . ."); *see also id*. at 234–35 ("The confidential relation is a prime example of the courts' failure to utilize contract fundamentals in determining the existence and scope of a volitional relation. . . . [T]he confidential relation concept is a creation of a felt need for restitution where courts believe they cannot find contract.").

184. First Community Bank, N.A., and People's Community Bank, A Division of First Community Bank, N.A., Privacy Policy (2007), https://www.fcbresource.com/privacy_statement.cfm (last visited Aug. 24, 2007).

185. Brex v. Smith, 146 A. 34, 36 (N.J. Ch. 1929).

186. Burrows v. Superior Ct. of San Bernardino County, 529 P.2d 590, 596 (Cal. 1974).

187. Suburban Trust Co. v. Waller, 408 A.2d 758, 764 (Md. Ct. Spec. App. 1979).

188. Peterson v. Idaho First Nat'l Bank, 367 P.2d 284, 289 (Idaho 1961).

189. L. RICHARD FISCHER, EMERGING ISSUES IN THE WORLD OF FINANCIAL PRIVACY, CONSUMER FINANCIAL SERVICES LITIGATION, PLI ORDER NO. B0–00NC, at 347–50 (2000).

190. *Cf*. Woods, *supra* note 16, at 42–43 (conceding that "*Miller* remains the law for now").

Customers may place great stock in the sense of security generated by these statements because of their particular concern for financial privacy. A post-9/11 survey by *PC World* found customers to be more resistant to law enforcement access to their financial records (seventy percent of respondents) than their internet use (sixty-three percent) or even their medical records (sixty-four percent).[191] A contemporaneous Harris poll also found that more Americans supported face-recognition technology to scan for suspected terrorists than closer monitoring of financial transactions.[192]

Privacy agreements between banks and customers currently espouse one of four variations in language, ranging from the most seemingly lenient ("as permitted by law") to the extremely narrow ("as compelled by law").

a. Bank-Customer Agreements Using Permissive Language

In its privacy policy, Sovereign Bank articulates: "We may share certain customer information with government and consumer reporting agencies as permitted or required by such laws as the Federal Right to Financial Privacy Act."[193] Similarly, Bank of America states: "We also may disclose . . . Customer Information to credit bureaus and similar organizations and when required or permitted by law."[194] The phrase "as permitted" has been interpreted narrowly by courts.[195] When a bank

191. Frank Thorsberg, *PC World Poll Highlights Privacy Concerns*, PCWORLD.COM (October 5, 2001), http://www.pcworld.com/article/id,64824-page,1/article.html (last visited Aug. 24, 2007).

192. *Id.*

193. *E.g.*, Sovereign Bank Privacy Policy and Interactive Reporting & Initiation Services (IRIS) Account Security Overview 5 (2007), http://www.sovereignbank.com/corporate/downloads/cashmanagement/inforeporting/irisprivacyandsecurity.pdf; Bryant Bank, Privacy Statement (2005), http://www.bryantbank.com/index.asp?page=951 ("Bryant Bank will safeguard your nonpublic personal information and will not sell or share any of your nonpublic personal information, except as provided in this Privacy Policy and Notice or as otherwise required by law.").

194. Bank of America Privacy Policy for Consumers 2007, http://www.bankofamerica.com/privacy/index.cfm?template=privacysecur_cnsmr (last visited Aug. 24, 2007); Chevy Chase Bank Privacy Pledge, http://www.chevychasebank.com/htm/privacy.html (last visited Aug, 24, 2007) ("We do not disclose any non-public personal information about our customers to any other third parties, except as permitted or required by law."); Citizens Bank, Notice of Citizens Privacy Pledge: Our Pledge to You Regarding the Responsible Use and Protection of Customer Information (Sept. 1, 2006), http://www.citizensbank.com/security/privacy.aspx (last visited Aug, 24, 2007) ("You do not have to respond to this notice in any way because we share your information only as permitted by law or as expressly authorized by you.").

195. *E.g.*, United States v. Terrey, 554 F.2d 685 (5th Cir. 1977); Peoples Bank of the Virgin Islands v. Figueroa, 559 F.2d 914 (3d Cir. 1977); West v. Costen, 558 F. Supp. 564 (W.D. Va. 1983).

contracts that it will disclose customer information only when "permitted" by law, it may not infer permission when the law is silent; rather, express authorization is necessary.[196] For example, the Federal District Court for the Western District of Virginia held that the collection of a service charge by a debt collector, which was not prohibited under state law, did not fit within the confines of the "permitted by law" exception since this conduct was not explicitly sanctioned by Virginia law.[197] This language has been interpreted in other contexts to limit bank discretion and proscribe the bank's choice of law.[198] Analogously, language permitting a party to disclose confidential information during legal proceedings is also construed narrowly. For example, courts have held that "[t]he Agreement may be interpreted strictly to require that the confidential information be used only in a court, not in settlement talks."[199]

Other banks claim that they will not disclose customer information except "when authorized by law."[200] For example, Jackson State Bank notes in its privacy statement, "[w]e do not disclose any non-public personal information about you to any non-affiliated third party unless authorized by you or we are authorized to do so by law."[201] This language is adopted by the Right to Financial Privacy Act, which provides that a subpoena may be issued when it "is authorized by law and there is reason to believe that the records sought are relevant to a legitimate law enforcement inquiry."[202] This language has generally been interpreted in favor of disclosure, giving considerable deference to law enforcement authorities.[203] Under the GLBA, banks are authorized to disclose customer information:

196. *West*, 558 F. Supp. at 582.

197. *Id.*

198. *Terrey*, 554 F.2d at 693 (holding that United States Small Business Administration had a duty to dispose of property in a commercially reasonable manner and that "as permitted" clause was intended as to limit discretion); *Figueroa*, 559 F.2d at 917 (holding that a bank could not volunteer information or respond to unauthorized requests "without breaching duties of confidentiality and privacy in its dealings with its customers").

199. Interclaim Holdings, Ltd. v. Ness, No. 00C7620, 2001 U.S. Dist. LEXIS 17945, at *27 (N.D. Ill. Oct. 29, 2001).

200. *E.g.*, The Jackson State Bank & Trust Policy on Customer Confidentiality and Privacy of Information, http://www.jacksonstatebank.com/custserv/privacy.cfm (last visited Aug. 24, 2007) (describing a typical policy).

201. *Id.*

202. 12 U.S.C. § 3407(1) (2000 & West Supp. 2007).

203. Irani v. United States, 448 F.3d 507, 510 (2d Cir. 2006) ("The statute creates entitlements of 'narrow scope' and 'is drafted in a fashion that minimizes the risk that customers' objections to subpoenas will delay or frustrate agency investigations.'") (quoting SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 745–46 (1984)).

> [T]o comply with Federal, State, or local laws, rules, and other applicable legal requirements; to comply with a properly authorized … investigation or subpoena or summons . . . or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law.[204]

When the bank has received a subpoena or summons, courts generally find the bank to be "authorized" to comply even if the customer objects.[205] Courts have allowed banks to disclose such information despite acknowledging the duty of confidentiality.[206] In doing so, courts have ranked the duty of confidentiality as subordinate to the duty to comply with subpoenas and summons.[207] However, IRS subpoenas differ from FISA requests and NSLs because the statutory provisions authorizing IRS subpoenas do not permit the bank to challenge the request for records.[208]

---

204. 15 U.S.C. § 6802(e)(8) (2000 & West Supp. 2007).

205. Banks have been allowed to simply ignore customer opposition in complying with subpoenas. Chapman v. Solar, No. 6:05–cv–1789–Orl–18JGG, 2006 U.S. Dist LEXIS 68805, at *12, *17 (M.D. Fla. Sept. 8, 2006) ("'When faced with a petition to quash an IRS third-party summons, the government need not move to enforce the summons. Instead the government can rely on the voluntary compliance of third parties to effectuate the summons. . . . ' A summons issued to a third-party recordkeeper does not generally implicate a taxpayer's privacy rights.") (quoting Cosme v. IRS, 708 F. Supp. 45, 48 (E.D.N.Y. 1989)). Courts have typically found that banks "cannot be held liable for breach of a fiduciary duty or for violation of a customer's right of privacy because of complying with a valid IRS subpoena." Schaut v. First Fed. Savings & Loan Ass'n, 560 F. Supp. 245, 247 (N.D. Ill. 1983).

206. Banks may also comply with subpoenas even when they have agreed, under seemingly restrictive language, to disclose customer information only when "required by law." Jacobsen v. Citizens State Bank, 587 S.W.2d 480, 481 (Tex. Civ. App. 1979) (finding no breach of confidentiality by bank in complying with IRS summons despite customer's oral and written instructions to keep information confidential on the ground that federal law preempts the imposition of liability); *see also* Kansas Comm'n on Civil Rights v. Sears, Roebuck & Co., 532 P.2d 1263, 1275-76 (Kan. 1975) (upholding disclosure of credit information pursuant to administrative subpoena); Rush v. Maine Savings Bank, 387 A.2d 1127, 1128 (Me. 1978) (no implied contractual duty to delay compliance with an IRS summons when summons requests ordinary information about a loan); Rycroft v. Gaddy, 314 S.E.2d 39, 43 (S.C. Ct. App. 1984) ("Communications in judicial proceedings are absolutely privileged and are immune from an action for invasion of privacy.").

207. Dan L. Nicewander, *Financial Record Privacy—What Are & What Should Be the Rights of the Customer of a Depository Institution?*, 16 ST. MARY'S L.J. 601, 631 (1985).

208. "The validity of an IRS summons may come before a district court in one of two ways. . . .Under no circumstance, however, is a summoned party entitled to bring a proceeding to quash the summons." Judicial Review of a Summons, U.S. Attorneys' Tax Resource Manual 55B (Feb. 2007), http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title6/tax00027.htm. *Contra* 50 U.S.C.A. § 1861(f) (West Supp. 2007) (allowing banks to challenge FISA requests for customer records); 18 U.S.C.A. § 3511 (West Supp. 2007) (allowing banks to analogously challenge NSLs in court).

b. Bank-Customer Agreements Using Restrictive Language

Many courts have held that banks may not make any disclosures concerning a depositor's account without the express or implied consent of the customer absent compulsion by law.[209] For example, the Alabama state courts consider it "well settled" that a bank cannot disclose customer information absent consent unless compelled by law.[210] Some banks have also contracted to abide to this narrow standard of disclosure.[211] Notably, a subpoena is generally considered compulsion.[212] When served with a subpoena, the recipient may respond with a written objection or move to quash or modify the subpoena if it requires the disclosure of protected information.[213]

If the recipient objects, the serving party may not inspect or copy any of the requested records unless the court that issued the subpoena issues an order to compel the production. For example, in the case of a subpoena requesting "suspicious activity reports" from the Federal Deposit Insurance Commission ("FDIC"), the FDIC was required to challenge the subpoena because a court could not compel production of this confidential and sensitive data.[214] Hence, there is precedent for this

209. Suburban Trust Co. v. Waller, 408 A.2d 758, 764 (Md. Ct. Spec. App. 1979); *see also* Bond v. Slavin, 851 A.2d 598, 608 (Md. Ct. Spec. App. 2004) (bank improperly produced records other than those requested in subpoena without consent of customer); *see also* Peoples Bank of the Virgin Islands. v. Figueroa, 559 F.2d 914, 917 (3d Cir. 1977) (bank volunteering information breaches duty of confidentiality).

210. White v. Regions Bank, 729 So. 2d 856, 858 (Ala. Civ. App. 1998) (internal quotations omitted).

211. *See e.g.*, Privacy Policy Disclosure, Iowa State Bank & Trust Company (Sept. 2006), http://www.isbt.com/privacy.php.

212. *See* Raymond, *supra* note 155, at § 10 ("In ruling that the borrower could not recover from the bank for disclosures compelled in a trial from its employee, who responded to a subpoena duces tecum, the court ruled that when a witness is asked a question, and no objection is made thereto, or, if made, is overruled, it is the duty of the witness to answer and the witness is not charged with the duty of determining whether the information sought is relevant or material.") (discussing O'Coin v. Woonsocket Inst. Trust Co., 535 A.2d 1263 (R.I. 1988)). This is true in other relationships meriting privacy as well, such as patient-doctor confidentiality: "[A] professional's duty to maintain his client's confidences is independent of the issue whether he can be legally compelled to reveal some or all of those confidences." McCormick v. England, 494 S.E.2d 431, 434 (S.C. Ct. App. 1997) (discussing patient-doctor duty of confidentiality). In addition, in the patient-doctor context, agreements promising that information will not be disclosed unless "compelled by law" may be breached when justified by "compelling public interest or other justification," such as the public policy of protecting the welfare of children through disclosure by physicians. *Id.* at 437. Hence, courts often interpret the exceptions to these privacy agreements more broadly than the text of the provisions would suggest.

213. FED. R. CIV. P. 45(c)(3)(A)(iii).

214. Fed. Deposit Ins. Corp. v. Flagship Auto Ctr., No. 3:04CV7233, 2005 U.S. Dist LEXIS 9468, at *16 (N.D. Oh. May 13, 2005) (citing FED. R. CIV. P. 45(c)(2)(B)) (holding that a court could not compel production of "suspicious activity reports").

Article's argument that subpoenaed entities may be required to object to a subpoena to preserve the confidentiality of a third party's information. The main distinction between the case of the FDIC reports discussed above and customer financial records is the source of the obligation: the FDIC's obligations arise under statute while banks' obligations to their customers are creatures of contract. However, as discussed in the following Part, banking contracts are contracts of adhesion that should be interpreted as privately drafted laws.

3. Interpreting Bank-Customer Agreements as Contracts of Adhesion

Because bank-customer agreements are drafted by the bank and presented to customers on a take-it-or-leave-it basis, they are often considered contracts of adhesion. Since these contracts are not the result of a bargained-for exchange, they should be treated with heightened judicial scrutiny. The differences in bargaining power, knowledge, and experience between the two parties may lead customers to make decisions that are not fully informed or completely voluntary. As a result, some scholars recommend that standard form contracts should not be enforced unless they conform to legislative standards reflecting fairness and public preferences.

In a landmark paper, Todd Rakoff identified seven factors to consider in determining whether an agreement is a contract of adhesion: (1) the contract is printed as a standard form; (2) the contract is presented on a take it or leave it basis, implying little bargaining power; (3) there is no bargaining in fact; (4) the seller who drafted the contract is a monopoly; (5) the product being sold is of necessity to the buyer; (6) the seller is sophisticated while the buyer is unsophisticated; and (7) the buyer did not read or understand the terms.[215] With the arguable exception of (4), agreements signed by bank customers appear to share all of these characteristics. Banking agreements are drafted in advance by the financial institution and are presented as invariable. Courts and scholars have spoken to the essential role of banks to economic life in society.[216] Consolidating the factors into a simple litmus test, one scholar defines a contract of adhesion as "that which would be a contract except that no bargaining power really shapes it."[217] Historically, contracts of adhesion have generally been upheld, except in cases where the terms or circumstances fall within the traditional exceptions to enforceability

215. Todd D. Rakoff, *Contracts of Adhesion: An Essay in Reconstruction*, 96 HARV. L. REV. 1173, 1177 (1983).

216. Burrows v. Super. Ct. of San Bernadino Valley, 529 P.2d 590, 596 (Cal. 1974).

217. Arthur Allen Leff, *Contract as Thing*, 19 AM. U. L. REV. 131, 143 (1970).

such as fraud, inducement, or unconscionability.[218] More recently, courts have expanded upon these historic exceptions by also refusing to hold the adhered party to such a contract. "Where the other party has reason to believe that the party manifesting such assent would not do so if he knew that the writing contained a particular term, the term is not part of the agreement."[219] In such cases, courts have severed the one-sided term while enforcing the remainder of the contract.[220]

a. A Realistic Approach to Contracts of Adhesion

Traditional doctrine proposes that parties should be bound to contracts of adhesion: because the adherent had an opportunity to read, his agreement signifies assent to the terms.[221] However, this inference rests on a mistaken assumption about adherents, most of whom do not actually read or comprehend the presented terms. This behavior is not mere laziness on the part of customers; rather, it reflects rational behavior because the terms are not negotiable.[222] Drafters capitalize on this inherent limitation by supplementing the salient attributes of the contract with self-favoring terms.[223] Accounting for the predictably self-dealing behavior of the drafting party, one scholar posits that the traditional equitable gloss on contracts—fraud, duress, and unconscionability—are inadequate to regulate contracts of adhesion, analogizing: "[I]t's like bandaging a cut on a broken leg."[224] Given the utter lack of choice or ability to dicker the terms, contracts of adhesion should not be taken at face value to be enforceable.

218. *Id.* at 142–43; *see also* THOMAS H. OEHMKE, COMMERCIAL ARBITRATION §§ 9:1, 9:3–9:4 (2006) ("An agreement may be voided as a contract of adhesion where there are multiple offending procedural and substantive badges of unconscionability. . . . A contract of adhesion is not automatically voidable . . . unless the agreement is unreasonable and never meets the parties' expectations.").

219. RESTATEMENT (SECOND) OF CONTRACTS § 211(3) (1981).

220. *See, e.g.*, Williams v. Walker-Thomas Furniture Co., 350 F.2d 445 (D.C. Cir. 1965) (holding that a contract in which the customer was assumed not to have paid off any of the items on her credit account until she had paid off all of the items "shocked the conscience" of the court).

221. Rakoff, *supra* note 215, at 1184 (citing Lewis v. Great Western Railway, 5 H. & N. 867, 157 Eng. Rep. 1427 (Ex. 1860)); *see also* Rakoff, *supra* note 215, at 1185–87 (discussing and critiquing the historic approach); KARL LLEWELYN, THE COMMON LAW TRADITION: DECIDING APPEALS 370 (1960) (arguing that blanket assent can be inferred from agreement because of the signor's opportunity to read).

222. Russell Korobkin, *Bounded Rationality, Standard Form Contracts, and Unconscionability*, 70 U. CHI. L. REV. 1203, 1203 (2003) (observing that, in reality, customers "are boundedly rational decisionmakers" who will normally price only "a limited number of product attributes" as part of their purchase decision).

223. *Id.* at 1203.

224. Leff, *supra* note 217, at 148.

b. Contracts of Adhesion as Private Lawmaking Meriting Judicial Scrutiny

Standard form contracts can be analogized to privately made law because they impose legally enforceable duties.[225] Lawmaking by private entities like financial institutions is non-majoritarian and clearly non-democratic. Regulations promulgated by such a process are legitimate only if they conform to standards that are arrived at democratically and reflect the public interest. This principle is prevalent with regard to administrative agency decisions, which are upheld only when they conform to intelligible principles set forth by the democratically elected Congress.[226] Whether contracts of adhesion conform to publicly determined standards is a helpful heuristic to figure out whether they should be enforced. As one commentator has argued, requiring conformity to such standards would serve public welfare because the standards would be based on the factors considered most relevant by customers and industry groups.[227] Along with fears of self-dealing and one-sided terms, comparative institutional competence may also favor delegating the allocation of risks to popularly elected bodies: "Legislatures are likely to be more institutionally competent to consider the preferences of the entire range of contracting parties than judges who . . . consider[] individual disputes."[228] For contracts of adhesion to be enforceable under a public law framework, it is necessary to establish the legitimacy of delegating some lawmaking to private parties.

In the case of bank-customer relations, Congress has legislated to hold banks to duties beyond those which banks freely assume in their dealings with customers.[229] As a matter of public policy, banks must keep customer information confidential outside of particular enumerated

225. W. David Slawson, *Standard Form Contracts & Democratic Control of Lawmaking Power*, 84 HARV. L. REV. 529, 530 (1971).

226. *See* Amalgamated Meat Cutters v. Connally, 337 F. Supp. 737 (D.D.C. 1971) (holding that the statute did not breach the non-delegation doctrine because the delegation of legislative authority was not absolute as it was limited by time, required subsidiary administrative policy allowing for assessment by public and courts of adherence to legislative intentions, enabled meaningful judicial review, and was required to be fair, generally applicable, and equitable). *But see* Schecter Poultry v. United States, 295 U.S. 495 (1935) (invalidating a statute for violating the non-delegation doctrine for delegation of authority to private individuals coupled with a lack of procedural safeguards or substantive standards of judicial review).

227. Slawson, *supra* note 225, at 536.

228. Korobkin, *supra* note 222, at 1249.

229. *See supra* Part III.B (discussing the attempts by Congress to expand privacy protections for personal information through the Right to Privacy Act of 1978 and the Gramm-Leach-Bliley Act of 1998).

exceptions.[230] Judicial review is essential to determining whether individual contracting systems conform to such legislative standards. Although courts typically uphold contracts unless their provisions are egregious enough to be considered fraudulent, induced, or unconscionable,[231] courts should apply a more scrutinizing standard of review to contracts likened to private lawmaking. One argument in favor of a more critical approach to contracts of adhesion is that in striking down contracts of adhesion, courts would not be striking a blow to freedom of contract generally because of the peculiar and coercive means by which these agreements were entered into.[232]

Contracts are based on a meeting of the minds and embody the intentions of the contracting parties.[233] Hence, proponents of the critical approach encourage courts to parse contractual provisions closely to discern which ones reflect shared intent.[234] In enforcing contracts, courts generally honor the reasonable expectations of the parties.[235] Courts should be particularly cognizant of those expectations in cases of contracts of adhesion, where the written contracts with their lengthy standard-form language and non-dickered terms are uniquely unlikely to reflect what the adherent expected from the relationship. As one proponent recognizes, the context of a transaction, not merely the written language on a standard form, shapes the reasonable expectations of the parties.[236]

230. Symons, *supra* note 98, at 245 ("These obligations have been imposed based on a legislatively determined sense of fairness and reasonableness established to protect expectations or perceived needs.").

231. U.C.C. § 1–304 (2007) ("Every contract or duty within [the Uniform Commercial Code] imposes an obligation of good faith in its performance and enforcement."); *see also id.* at § 2–302 ("If the court as a matter of law finds the contract or any clause of the contract to have been unconscionable at the time it was made the court may refuse to enforce the contract.").

232. Slawson, *supra* note 225, at 541 (concluding that "[t]he standard form is not a contract").

233. ROBERT E. SCOTT & JODY S. KRAUS, CONTRACT LAW & THEORY 676 (3d ed. 2002)."Because parties incur contractual liability only if they make a voluntary, informed promise, contractual obligations can be said to arise out of the parties' consent. . . . [T]he autonomy and economic justifications of contract law presuppose a vital connection between the parties' intent and the obligations contract law enforces." *Id*.

234. Slawson, *supra* note 225, at 541.

235. *E.g.*, *id.* ("[O]nly the expressions, or manifestations, of consent of the contracting parties should be called the contract and should be enforced, generally, without question."); *see also* Allen v. Prudential Property & Cas. Ins. Co., 839 P.2d 798, 801 (Utah 1992) ("In general, the reasonable expectations doctrine authorizes a court confronted with an adhesion contract to enforce the reasonable expectations of the parties under certain circumstances."). *See generally* Roger C. Henderson, *The Doctrine of Reasonable Expectations in Insurance Law After Two Decades*, 51 OHIO ST. L.J. 823 (1990) (discussing that the reasonable expectations principle consists of applicable rules).

236. Slawson, *supra* note 225, at 544.

c. Particular Vulnerabilities of Contracts of Adhesion

The greatest discord between contractual provisions and customer expectations may be reflected in clauses expressing how the institution will behave in case of a particular contingency. Courts should exercise heightened vigilance in enforcing such contingent clauses because they are the least likely to be read or understood by customers since it is "notoriously difficult for most people, who lack legal advice and broad experience concerning the particular transaction type, to appraise these sorts of contingencies."[237] Of particular concern with regard to disclosure provisions is that customers are likely to ignore or undervalue risks with a low probability of occurrence because they are unrealistically confident in their ability to escape harm.[238] The risk of being suspected or targeted in a counterterrorism investigation is perhaps as unfamiliar or unimaginable to most people as it comes. Hence, customers will systematically undervalue any protections proffered by banks ex ante and are unlikely to notice when banks grant themselves considerable leeway to disclose customer information to law enforcement authorities.[239]

Knowing that customers lack the willingness and ability to evaluate contingent terms such as disclosure procedures, banks realize that only a few terms will engage customer attention and need to be drafted in a favorable manner.[240] As a result, the adhering party is "frequently not in a position to shop around for better terms, either because the author of the standard contract has a monopoly (natural or artificial) or because all competitors use the same clauses."[241] To the extent that courts uphold such terms, they are merely sanctioning the "[u]se of form contracts [which] enables firms to legislate in a substantially authoritarian manner" without any political accountability.[242] Instead of espousing a uniform presumption of enforceability or

237. Rakoff, *supra* note 215, at 1226.

238. Korobkin, *supra* note 222, at 1232–33 ("[P]eople often assess risk via the 'availability heuristic,' judging risk to be high when the type of harm is familiar or easily imagined and low when it is not."). *Contra* Andrew Kull, *Mistake, Frustration & the Windfall Principle of Contract Remedies*, 43 HASTINGS L.J. 1 (1991–92) (arguing that courts may not be any more well-positioned to allocate risks of unexpected contingencies than the parties drafting the contracts).

239. *Contra What Price Privacy?*, CONSUMER REPORTS, May 1991, at 356 ("There's no conspiracy afoot to deny Americans their rights or start Big Brotherish monitoring of our activities. Instead, privacy is being slowly eroded. 'The potential threat is large. . . . But it's hard for people to get worked up about it because the erosion is usually quite subtle.'").

240. Korobkin, *supra* note 222, at 1225–27.

241. Friedrich Kessler, *Contracts of Adhesion—Some Thoughts About Freedom of Contract*, 43 COLUM. L. REV. 629, 632 (1943).

242. *Id.* at 640.

unenforceability of form contracts, some commentators favor a more nuanced approach under which the legal response would depend on the "social importance of the contract" and the "degree of monopoly enjoyed by the author."[243]

Instead of conditioning enforceability on conformance to societal, democratically-developed standards, a more draconian appriach to contracts of adhesion is considering adhesive terms to be presumptively unenforceable. This approach has been proposed by one scholar who questions judicial deference to adhesive contracts in light of who their drafters are, noting that "[b]usiness firms do not much resemble the types of voluntary organizations to which the law gives great deference."[244] This suggests that judicial review, either under the historic deference to contracts of adhesion or even under heightened scrutiny may be insufficient to efficiently protect customer expectations. The two approaches may often lead to a shared outcome since "many of the terms in typical form documents are specifically designed to displace clear rules of law that would otherwise govern the transaction"[245] and such terms would not be upheld under a litmus test of conformance. One possible middle ground may be to treat contracts of adhesion as informative in determining parties' rights rather than directly enforceable on their terms; standard forms and the expert judgments they reflect could be treated as "possible evidence of what the legally implied terms should be, rather than as an independent basis for enforcement."[246]

Critics of contracts of adhesion acknowledge that forcing institutions to abide by socially sanctioned terms, which they may gloss over by drafting contracts in a vague or complex manner in a more permissive regime, may result in higher prices.[247] However, many prefer higher prices over enforcement of contracts that do not conform to customer expectations.[248] As one might infer, "[i]f the point is that onerous terms are justified by an apparent consumer preference for low prices, it rests on a failure to perceive the institutional dynamic that leads adherents to focus exclusively on visible terms."[249]

243. *Id.* at 642.

244. Rakoff, *supra* note 215, at 1240 (arguing that considering standard-form contracts to be presumptively enforceable would not endanger freedom of contract among individuals).

245. *Id.* at 1183.

246. *Id.* at 1247.

247. Korobkin, *supra* note 222, at 1260.

248. Rakoff, *supra* note 215, at 1247.

249. *Id.* at 1264.

4. Banks as Private Enterprises Drafted into Law Enforcement by the State

Courts often police bank-customer agreements that give banks wide discretion to disclose customer information to commercial entities such as marketers. In contrast, courts are more deferential to privacy agreements that permit the bank to disclose customer information to government entities. However, agreements that allow banks to disclose customer information to law enforcement authorities should also be judged with heightened scrutiny because customers may not have willingly and knowingly agreed to the terms. Policymakers have not clarified why the government is covertly soliciting this information from banks rather than acting publicly as its own agent subject to the controls of the electorate.

On one hand, the government may be wary of soliciting private sector firms such as banks to collect information about its citizens because society is often more skeptical of the motives of profit-maximizing corporate entities.[250] However, since the collection and dissemination of information does not appear to be closely linked to any profit-making end, it seems unlikely that there would be any greater skepticism toward the motives of a private rather than public entity. Furthermore, since customers are not notified when their records are solicited, the private institutions remain largely immune from public criticism.[251] Allowing the government to draft private enterprise into its national security operations without publicly acknowledging this partnership is particularly dangerous because, unlike market-regulated private entities, the government may be cavalier about the risks involved in its behavior, justifiying its actions as "in the public interest" despite the potentially adverse effects.[252]

250. Christopher D. Stone, *Corporate Vices & Corporate Virtues: Do Public/Private Distinctions Matter?*, 130 U. PA. L. REV. 1441, 1459 (1982) ("A different quality or depth of indignation might be aroused by the company that hazards health 'for profit' than by the public laboratory that does so in the pursuit of science, and whose successes would be more ratably shared among the whole population.").

251. 50 U.S.C.A. § 1861(d)(1) (West Supp. 2007).

252. Stone, *supra* note 250, at 1459 (citing the Tuskeegee study in which syphilis was "studied" instead of cured and the leukemia exposures from testing nuclear weapons); *see also* Cal. Bankers Ass'n v. Schultz, 416 U.S. 21, 66 (1974) ("It is conceivable, and perhaps likely, that the bank might not of its own volition compile this amount of detail for its own purposes, and therefore to that extent the regulations put the bank in the position of seeking information from the customer in order to eventually report it to the Government."). *But see id.* at 48–49 ("Banks are therefore not conscripted neutrals in transactions involving negotiable instruments, but parties to the instruments with a substantial stake in their continued availability and acceptance.").

Privatization can be a strategic move to avoid the high visibility that accompanies overt state action. After all, public awareness may well be followed by an unfavorable response by the electorate.[253] The government is considered an agent subject to control by the public, unlike private organizations such as financial institutions. For example, a program that explicitly required individuals to report all of their financial transactions to a central data-gathering government agency would create a much greater public outcry than a government policy of secretly requesting the same information from banks.[254] By implementing an indirect program, the government is capitalizing on the difficulties any principal (in this case the public) faces in monitoring its agent (in this case the government), particularly when the agent's actions are shrouded in confidentiality and outsourced to complicit private entities.[255]

Furthermore, non-compulsory NSLs are being issued by agencies that could not get access to records through the usual avenues of inter-agency cooperation or congressional mandate.[256] This may reflect the reality that it is often easier for a public agency to change the behavior of a private organization than of another public agency.[257] However, the fact that the CIA and DoD could not obtain congressional backing

253. Stone, *supra* note 250, at 1467 (noting that the public may be less keen on punishing government entities because the penalties would be drawn from taxpayers' pockets).

254. For example, the government long kept its phone monitoring program under wraps. ABC News: Good Morning America, *Government Monitoring About 200 Million Phone Calls*, (May 11, 2006), http://www.abcnews.go.com/GMA/story?id=1948927&page=1 ("In all their comments about the eavesdropping program, U.S. officials never revealed that they were involved in this massive collection of telephone data."). When word of government surveillance leaks, it is generally met with opposition from public watchdog groups. In response to the FBI's "Carnivore" program, which monitors email traffic and can intercept the email of criminal suspects, the Electronic Privacy Information Center filed suit challenging its legality. Complaint 5–6, Electronic Privacy Info. Ctr. v. Dep't of Justice, No. 00-CV-1849 (D.D.C. July 31, 2000), *available at* http://www.epic.org/privacy/carnivore/complaint.pdf (citing *FBI's System to Covertly Search Email Raises Privacy, Legal Issues*, WALL ST. J., July 11, 2000).

255. Robert Schmul, *Government Accountability & External Watchdogs*, ISSUES OF DEMOCRACY 21, 24 (Aug. 2000), *available at* http://usinfo.state.gov/journals/itdhr/0800/ijde/ijde0800.pdf.

256. *See supra* Part II.C (discussing the ability of the CIA, Department of Defense, and other agencies to issue voluntary NSLs).

257. J.Q. Wilson & P. Rachal, *Can the Government Regulate Itself?*, THE PUB INTEREST 3–4 (Winter 1977); Stone, *supra* note 250, at 1502 ("[T]he tendency suggests special reason for courts to consider suspect any legislation that concentrates the costs of exemplary behavior on subgroups, and away from the government.").

for their NSLs implies something about the political unwillingness of elected parties to support this scheme.[258]

By masking the gathering of information with nondisclosure requirements that prevent banks from notifying customers that their records have been requested, the government has largely evaded the heightened scrutiny that courts apply to state action.[259] It is possible that a strategic move to privatize information collection in order to avoid judicial inference of constitutional obligations would be ineffective because the courts could easily look beyond the nominally private actor to discern the underlying state actor.[260] However, this veneer of private action can be quite effective since courts are, in practice, often reluctant to reclassify private actors as essentially public.[261]

Nonetheless, judicial control is particularly essential in the financial privacy context because the public is ill-equipped to effectively monitor government activity.[262] Courts are the only entities informed of FISA requests and NSLs, and banks bring challenges in only the minority of cases. Hence, judicial remedies must supplement the political processes

258. *See supra* Part II.C (discussing Congress's reluctance to grant these agencies powers to aid in domestic spying).

259. Stone, *supra* note 250, at 1483 ("[I]f the courts find state action, some constitutional standards of conduct become obligatory . . . [and] the courts, having a constitutional basis for their review, are likely to exercise more scrutiny."); *see, e.g.*, Owen v. City of Independence, 445 U.S. 622, 638 (1980) (holding that a municipality has no immunity from liability under the Civil Rights Act flowing from its constitutional violations and may not assert the good faith of its officers as a defense to such liability).

260. For example, in § 1983 actions, private actors sometimes engage in state action when they act in concert with government officials. *E.g.*, West v. Atkins, 487 U.S. 42, 57 (1988) (holding that a private physician who treated prison inmates in a state facility was engaging in state action); *see also* Pennzoil Co. v. Texaco, Inc., 481 U.S. 1, 1 (1987) (holding that a creditor invoking the state's judgment-enforcement mechanism may be considered a state actor).

261. For example, the Supreme Court refused to find state action in the case of a "private" school that almost solely provided specialized teaching services under a government contract. Rendell-Baker v. Kohn, 457 U.S. 830, 840–44 (1982). The Court failed to find that school officials were acting under color of state law. *Id.* Consequently, the Court denied the teachers' § 1983 civil rights claims. *Id.* at 836.

262. Stone, *supra* note 250, at 1469 ("Because monitoring and controlling by political process thus have their own limitations, at some point it makes sense to shift toward judicially imposed liabilities."). However, the Supreme Court has previously considered the constitutionality of the record maintenance and reporting requirements of the Bank Secrecy Act and declined to find violations of the First, Fourth, Fifth, or Fourteenth Amendments. *E.g.*, Cal. Bankers Ass'n v. Schultz, 416 U.S. 21 (1974) (holding that record-keeping requirements imposed by Secretary's regulations did not deprive banks of due process by imposing unreasonable burdens upon them; that the mere maintenance of records by the banks under compulsion of the regulations does not constitute seizure; and that the association's claim that record-keeping requirements violated its members' First Amendment rights were premature where the government had not sought disclosure of the association's membership and contributors).

that generally serve as a check on state actors. The Supreme Court previously considered the claim that "when a bank makes and keeps records under compulsion of the Secretary's regulations it acts as a Government agent and thereby engages in a seizure of its customer's records."[263] However, in that case, determining the constitutionality of the 1970 Bank Secrecy Act, the Court held that because the banks were merely maintaining records and disclosing transactions to the government when faced with a subpoena, there was no illegal search or seizure.[264]

IV. OPPORTUNITIES AND OBLIGATIONS TO CHALLENGE LAW ENFORCEMENT INQUIRIES

The obligations of banks to their customers—whether mandated by statute or invited by contract—prevent banks from exercising full discretion in actions implicating customer privacy. Although banks must respect the authority of law enforcement agencies, they should also act in accordance with the reasonable expectations of their customers rather than merely abiding by the most lenient reading of the contracts of adhesion they draft. While notions of confidentiality generally inform the bank-customer relationship, how a bank should act when called on to divulge customer information in a particular instance depends on the type of request, the nature of the relationship, and the jurisdiction.

As discussed above, neither the FISA nor the NSL statute, in giving banks the power to object to law enforcement inquiries, require the exercise of this newly granted authority.[265] However, customers expect that banks will guard their information and protect their privacy.[266] This expectation is an essential part of the bank-customer relationship as encouraged by bank statements, understood by both customers and courts, and embodied in the privacy agreements that banks draft for

263. *Cal. Bankers Ass'n*, 416 U.S. at 22.

264. *Id. at* 54 ("That the bank in making the records required by the Secretary acts under the compulsion of the regulation is clear, but it is equally clear that in doing so it neither searches nor seizes records in which the depositor has a Fourth Amendment right.").

265. However, the FISA and NSL contexts are unique from other forms of government requests for records, such as IRS subpoenas. As courts have noted, the statutory scheme governing IRS subpoenas, by contrast, do not contain any "legally recognized privilege entitling the bank to withhold such records on behalf of its depositor." Hence, in the case of an IRS subpoena, "[t]he bank must cooperate with the summons even in the absence of a court order." Jacobsen v. Citizens State Bank, 587 S.W.2d 480, 481 (Tex. App. 1979) (citing United States v. Bremicker, 365 F. Supp. 701 (D. Minn. 1973) (discussing IRC § 7602 (2007)).

266. *See supra* Part III.C.1.a (discussing the duty of confidentiality recognized in the bank-customer relationship at common law).

their customers to sign.[267] While providing a general guarantee of privacy, these agreements contain exceptions allowing the bank to disclose customer records in response to law enforcement inquiries. Courts have typically construed these exceptions narrowly but granted great deference to law enforcement in allowing banks to release customer information.[268]

However, allowing banks to disclose customer information whenever permitted by the plain language of the bank-customer agreements does not account for the fact that these agreements are contracts of adhesion. Because the agreements were drafted en masse by the financial institution and presented to the adherent on non-negotiable terms, they do not necessarily reflect the intent or even the assent of the customer.[269] Given the circumstances surrounding their origin, the precise language of bank-customer agreements should not be entitled to deference unless it conforms to democratically-determined standards,[270] namely the respect for financial privacy reflected by congressional enactments such as the RFPA, GLBA and, more recently, the Reauthorized Patriot Act with its new focus on the importance of pre-enforcement.

A. Type of Law Enforcement Inquiry

Bank-customer agreements uniformly permit banks to disclose customer information under compulsion by law.[271] Courts have generally considered subpoenas to be compulsion, valuing bank compliance with law enforcement over customer confidentiality.[272] In other contexts, courts tend to be deferential to subpoenas when ruling on a motion to quash.[273] However, this Part will argue that the unique

267. *See supra* Part III.C.2 (discussing explicit terms in bank privacy policies and the fiduciary duties recognized in the bank-customer relationship).

268. *See supra* notes 174–76 (discussing case law involving breaches of customer privacy by banks).

269. Slawson, *supra* note 225, at 544.

270. Symons, *supra* note 98, at 244.

271. Privacy Policy Disclosure, Iowa State Bank & Trust Company (Sept. 2006), *available at* http://www.isbt.com/privacy.php; The Jackson State Bank & Trust Policy On Customer Confidentiality and Privacy of Information, *available at* http://www.jacksonstatebank.com/custserv/privacy.cfm; Bank of America Privacy Policy for Consumers 2007, *available at* http://www.bankofamerica.com/privacy/index.cfm?template=privacysecur_cnsmr.

272. *E.g.*, White v. Regions Bank, 729 So. 2d 856, 858 (Ala. Civ. App. 1998) (noting that banks cannot disclose customer information without the customer's consent, unless through compulsion by law) .

273. *E.g.*, Rush v. Maine Sav. Bank, 387 A.2d 1127, 1128 (Me. 1978) ("[T]here is no implied contractual duty on the part of a mortgagee-bank to delay compliance with an I.R.S. summons, at least when the summons requests ordinary information.").

circumstances surrounding FISA requests for records and NSLs warrant greater judicial scrutiny. FISA section 215 requests lack the ex ante and ex post procedural safeguard of warrants. NSLs lack even the minimal safeguards that the FISA process mandates for section 215 requests because the agency need not seek judicial approval prior to issuance.[274]

1. FISA Section 215 Requests

a. FISA Section 215 Requests Lack the Ex Ante Procedural Safeguard of Warrants

Upon first examination, effectuating a request for documents under section 215 looks similar to obtaining a search warrant because both require judicial approval.[275] However, a closer look at the FISA request process reveals that the judicial role should be regarded as more of a ministerial nod of approval than a critical eye. Although applications for FISA "warrants" are reviewed by specially selected federal judges, these judges are given only minimal criteria on which to evaluate the appropriateness of the applications.[276] Rather than the showing of probable cause typically required to obtain a search warrant, the applicant need only show that the records are sought for a foreign intelligence, clandestine, or international terrorism investigation.[277] The ACLU has argued that "[a]s a result of the changes effected by the Patriot Act, the FBI is now authorized to use section 215 even against people who are known to be altogether unconnected to criminal activity or espionage."[278]

Furthermore, the agency is not required to show any special need for secrecy when requesting a clandestine search.[279] Although a court order is technically required under FISA, the judge has limited opportunity to engage in meaningful review of the agency's decision.[280] These emaciated judicial protections are coupled with greater flexibility

274. Rosen, *supra* note 39 ("National security letters are especially susceptible to abuse because they're not subject to independent review by a judge or magistrate and because the recipients are forbidden to discuss them.").

275. *See supra* Part II.B (explaining the process for acquiring NSLs).

276. Schulhofer, *supra* note 84, at 533.

277. Complaint for Declaratory & Injunctive Relief at 6–7, Muslim Comty. Ass'n of Ann Arbour v. Ashcroft, 459 F. Supp. 2d 592 (E.D. Mich. 2006) (No. 03–CV–72913–DT), *available at* http:// fl1.findlaw.com/news.findlaw.com/hdocs/docs/aclu/mcaa2ash73003cmp.pdf (noting former Attorney General John Ashcroft's testimony that the "reason to believe that the target is an agent of a foreign power" standard may be said to be "lower than probable cause").

278. *Id.* at 6.

279. Schulhofer, *supra* note 84, at 544.

280. *Id.* at 533.

in investigative procedures than is typically permitted in conventional criminal investigations. Perhaps most notably, FISA authorizes clandestine search tactics that prevent the suspect from being notified.[281] Even if the suspect is eventually prosecuted, the defense attorney is not usually permitted to review the associated surveillance documents.[282] In addition, FISA searches may be authorized for broader timelines with less judicial supervision than in conventional investigations.[283]

There are also fewer ex post safeguards following the search or surveillance than in a conventional investigation. Judicial review at the completion of the surveillance action is merely optional.[284] Those subjected to clandestine searches may never be notified unless they are eventually prosecuted, making it effectively impossible to obtain remedies for unwarranted intrusions into privacy even though the Patriot Act provides for a civil damages scheme.[285] As one commentator concluded: "In all of these respects, the FISA regime offers far less accountability and thus a greatly enhanced risk of abuse."[286]

Since the specific reports of the Foreign Intelligence Surveillance Court ("FISC" or "FISA Court") regarding individual applications are not publicly released, it is difficult to assess how closely the applications are reviewed. While the aggregate numbers indicate that the court has been playing a more active role since the passage of the 2001 Patriot Act, over ninety-nine percent of applications are

281. Michael J. Bulzomi, *Foreign Intelligence Surveillence Act*, 72 LAW ENFORCEMENT BULL. 6, 30 (June 2003), *available at* http://www.fbi.gov/publications/leb/2003/june03leb.pdf (citing 18 U.S.C. § 3103(a) (2000)) ("Delayed notice, or sneak-and-peek warrants, are now permissible where the court finds reasonable cause to believe that immediate notification of the execution of the warrant would have an adverse result.").

282. Schulhofer, *supra* note 84, at 544.

283. *Id.* at 534.

284. 50 U.S.C.A. § 1805(e)(3) ("At or before the end of the period of time for which electronic surveillance is approved by an order or an extension, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.")

285. 18 U.S.C.A. §§ 2520(g), 2707(g) (West Supp. 2007) (imposing civil liability on investigative or law enforcement officers or entities of the government for any willful use or unauthorized disclosure of information); 18 U.S.C.A. § 2712(a) (West Supp. 2007) (creating a cause of action against the United States for victims of willful violations of the FISA requirements relating to surveillance or physical searches). *But see* Schulhofer, *supra* note 84, at 542–43 ("But the civil remedy is virtually meaningless because those individuals, unless subsequently prosecuted, can virtually never learn that they had been under surveillance.").

286. Schulhofer, *supra* note 84, at 538.

approved.[287] Before 2001, the FISA Court received about 750 applications per year and had never rejected a single one.[288] In 2003, the FISA Court reviewed 1724 applications and denied only four. These numbers have led notable civil liberties groups to refer to the FISA Court as a rubber stamp.[289] Before 9/11, the FBI was required to certify that the records were sought for a foreign intelligence purpose and that "specific facts" confirmed that the records pertained to the agent of a foreign power.[290] In the 2001 Patriot Act, both of these requirements were eliminated and replaced by a good-faith standard.[291] Furthermore, the FISA Court has a very limited and deferential standard of review and lacks statutory authority to examine or reject the FBI's certification that the records are sought for an investigation related to foreign intelligence or terrorism.[292]

b. FISA Section 215 Requests Lack the Ex Post Procedural Safeguards of Subpoenas

During the discovery phase of conventional civil litigation, private litigants may issue subpoenas without prior judicial approval.[293] Unlike bank customers whose records are subpoenaed by FISA requests, recipients of conventional civil subpoenas in private litigation are notified of the document production request and have an opportunity to challenge it in court by filing a motion to quash the subpoena.[294] Hence, "the recipient of a subpoena gets a procedural option not available to the target of a search: she can challenge the subpoena prior to releasing the information."[295] The recipient may file a motion to quash and receive a hearing in front of a judge.[296] Although the requirements for upholding a subpoena are minimal, "judicial oversight, even in this highly diluted form, does act as a check on unrestricted

287. EPIC, FISA Orders 1979–2006, http://www.epic.org/privacy/wiretap/stats/fisa_stats.html (last visited Aug. 27, 2007).

288. *Id.*

289. Timothy Edgar & Witold Walczak, *We Can Be Both Safe & Free: How the PATRIOT Act Threatens Civil Liberties*, 76 PA. B. ASS'N Q. 21, 22 (2005) ("[T]he PATRIOT Act in some cases eliminates judicial review entirely, through national security letters for instance, and in many instances changes the review standard to make judges little more than rubber stamps.").

290. Schulhofer, *supra* note 84, at 548–49.

291. *Id.* at 549 ("It is no longer necessary for the FBI to have factual support for its decision to investigate, and it is not even necessary for agents to believe that the targeted person is a suspected offender or a foreign agent.").

292. 50 U.S.C.A. § 1861(c)(1) (West 2003 & Supp. 2007).

293. FED. R. CIV. P. 45(a)(3).

294. *Id.* at 45(c)(3)(A).

295. Schulhofer, *supra* note 84, at 545.

296. *Id.*

official snooping, and it provides the subpoena recipient an important guarantee of accountability."[297] Furthermore, judicial oversight may be particularly influential in the arena of financial privacy, because courts are reluctant to compel the discovery of personal financial records. Courts typically decline to uphold subpoenas for financial information in civil suits, failing to find such inquiries relevant under normal circumstances.[298]

By contrast, in the case of a FISA request, the customer is never notified of the subpoena and hence has no ability to contest it.[299] Unless banks challenge these subpoenas, there is no judicial inquiry into the basis of the investigation and the necessity of the intrusion into the customer's privacy.[300] This is particularly disturbing because judicial review has been called "the most common and important civil liberties protection."[301]

2. National Security Letters Lack Even the Procedural Protections of FISA Requests

The NSL process lacks even the minimal judicial safeguards mandated by the formalistic FISA request procedure. To issue an NSL, the agency need not seek judicial approval prior to enforcement.[302] Courts only enter the process if the recipient of the letter petitions to have the letter modified or set aside.[303] Since customers are not the recipients of the letters and do not receive notice, they rely on banks to involve courts when necessary. Indeed, banks serve as the gatekeepers to judicial review of NSLs.

Banks should take it upon themselves to challenge NSLs or at least to review the letters in order to make a reasoned determination as to whether a challenge may be necessary. While a subpoena may be considered compulsion of law and many bank agreements explicitly mention subpoenas as an exception to nondisclosure requirements, this

297. *Id.*

298. Jack W. Campbell IV, *Revoking the "Fishing License": Recent Decisions Place Unwarranted Restrictions on Administrative Agencies' Power to Subpoena Personal Financial Records*, 49 VAND. L. REV. 395, 432 (1996); *e.g.*, Sanderson v. Winner, 507 F.2d 477, 479 (10th Cir. 1974) ("Ordinarily courts do not inquire into the financial responsibility of litigants. We generally eschew the question whether litigants are rich or poor."). *But see* FED. R. CIV. P. 69(a) (allowing compulsion of financial records to enforce a judgment).

299. Schulhofer, *supra* note 84, at 554.

300. *Id.* (stating that bank inaction also eliminates "virtually any possibility for public criticism").

301. Edgar & Walczak, *supra* note 289, at 22.

302. Rosen, *supra* note 39.

303. 18 U.S.C.A. § 3511 (West Supp. 2007).

exception should not be interpreted to include NSLs.[304] Furthermore, most federal cases holding that a depositor has no proprietary interest in his bank records, and consequently no standing to challenge the solicitation of his records by law enforcement authorities under the Fourth Amendment, involve customers resisting formal subpoenas or summons authorized by administrative or judicial bodies, not merely informal requests.[305] Non-mandatory NSLs are not backed by a comparable force of law—a judicially decreed order—unless they are challenged and subsequently upheld in court.[306] Hence, permissive compliance with NSLs does not fall within the strict confines of the "as compelled by law" language adopted by many banks in their privacy agreements.[307] Furthermore, blind acquiescence to the whims of law enforcement does not meld with case law in most states, which has limited the disclosure of customer records to authorities to subpoenas, summons, and other formal processes.[308] In addition, releasing records without examining the nature of the request or the requesting authority conflicts with banks' promises to respect customer privacy and their self-assigned duty of confidentiality.[309] This is particularly true when banks take on heightened obligations to their customers by serving in more intimate roles.[310]

304. 15 U.S.C.A. § 6802(e)(8) (2000 & West Supp. 2007).

305. *E.g.*, Interstate Commerce Comm'n v. Brimson, 154 U.S. 447, 485 (1894) (discussing the necessity for citizens to yield to summonses from the Interstate Commerce Commission); United States v. Gross, 416 F.2d 1205, 1212–13 (8th Cir. 1969) (determining bank and Western Union records to be admissible evidence, due to customers' lack of ownership); Harris v. United States, 413 F.2d 316, 317–18 (9th Cir. 1969) (explaining that the bank owned microfilms it made of checks, leaving no rights to the customer); Galbraith v. United States, 387 F.2d 617, 618 (10th Cir. 1968) (determining that bank records were solely the property of the bank). *But see* Vera Bergelson, *It's Personal But Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 443 (2003) (explaining that individuals should have options to "keep their personal information private , or conversely, sell, pledge, or license it").

306. 18 U.S.C.A. § 3511(c) (West Supp. 2007).

307. Winer, *supra* note 62.

308. *See supra* Part III.C.2.b (discussing when banks must disclose customer information).

309. In analogous contexts, banks have conditioned their deference to law enforcement authorities on the presence of a subpoena. For example, in holding that a bank must comply with a subpoena and its non-disclosure requirement despite its promulgated privacy policy, the Supreme Court of Kansas accorded considerable weight to the fact that the law enforcement request was a subpoena. State *ex. rel*. Brant v. Bank of Am. 31 P.3d 952, 959 (Kan. 2001).
In that case, the Commissioner of the Securities and Exchange Commission issued the subpoena, but judicial intervention was required for its enforcement: "The Commissioner's subpoena power is not self-executing. There is an avenue open to challenge the Commissioner's alleged abuse of his investigative powers." *Id*.

310. 12 U.S.C. § 1813(f) (2000) ("The term 'mutual savings bank' means a bank without capital stock transacting a savings bank business, the net earnings of which inure wholly to the benefit of its depositors after payment of obligations for any advances by its organizers."); Pigg v.

Courts should approach bank compliance with non-mandatory NSLs with the same skepticism they have toward voluntary disclosure in analogous contexts. The Court of Appeals for the Tenth Circuit has held that a bank cannot voluntarily disclose customer information to government authorities.[311] In finding that banks could not grant the IRS informal access to bank records, the court determined that voluntary cooperation does not exempt banks from the requirements of the RFPA.[312] Similarly, the California courts rejected the voluntary nature of the bank's disclosure as a defense to allegations of Fourth Amendment violations, reasoning that the customer "has a reasonable expectation of privacy in the bank statements, [and] the voluntary relinquishment of such records by the bank at the request of the police does not constitute a valid consent."[313]

Before the Intelligence Authorization Act of 1987, the FBI could only issue such non-mandatory letters.[314] A substantial number of financial institutions complied voluntarily.[315] However, as FBI officials testified to a House Committee that proposed the 1987 amendment, "in certain significant instances, financial institutions have declined to grant the FBI access to financial records in response to requests under § 1114(a) . . . particularly in States which have State constitutional privacy protection provisions or State banking privacy laws."[316] Financial institutions that did not comply with the letters claimed that "[s]tate law prohibit[ed] them from granting access and the RFPA, since it permits but does not mandate such access, does not override State law;" they feared that "cooperation might expose them to liability to the

Robertson, 549 S.W.2d 597, 600–02 (Mo. Ct. App. 1977) (implying a confidential relationship where bank employees were called upon to give advice to customers).

311. Neece v. IRS, 922 F.2d 573, 577–78 (10th Cir. 1990) ("The provisions of the RFPA provide an elaborate mechanism to protect a taxpayer's privacy rights in records kept by third parties. We must protect this mechanism.").

312. *Id.* at 578 ("We, therefore, hold that a financial institution and a Government authority . . . otherwise bound by the procedural requirements of the RFPA . . . are not exempted . . . from those procedural requirements merely because the financial institution voluntarily chooses to allow the IRS . . . to examine financial records pertaining to a taxpayer.").

313. Burrows v. Superior Court of San Bernardino County, 529 P.2d 590, 594 (Cal. 1975).

314. H.R. REP. NO. 99–690(I), sec. 403, at 14–15 (1986), *as reprinted in* U.S.C.C.A.N. 5327, 5340–41.

315. Palmer & Palmer, *supra* note 107, at 211.

316. H.R. REP. NO. 99–690(I), sec. 403, at 15. The House committee did not speak directly to the potential for liability under the original section 1114(a) but noted that the addition of section 404 would solve this noncompliance problem: "[B]y providing for mandatory FBI access to a customer's or entity's financial records for counterintelligence purposes in certain circumstances, [section 404] preempts State law to the contrary which otherwise would not permit such access." *Id*. at 16.

customer to whose records the FBI sought access."[317] The fact that Congress felt the need to amend the statute to make compliance mandatory in order to ensure that banks would not be liable for disclosing records in response to NSLs indicates that noncompulsory letters do not enjoy absolute priority over state privacy protections.

By passing the Intelligence Authorization Act of 1987, Congress clearly stated that mandatory NSLs supersede state privacy protections without addressing whether compulsory letters similarly take precedence over contractual obligations. However, by negative implication and from Congress's felt need to amend the statute to require compliance, it appears that Congress was not willing to claim that non-compulsory letters were entitled to the unwavering deference of banks. Given the tenuous authority and minimal procedural safeguards of non-compulsory NSLs, banks should not prioritize compliance over state constitutional provisions and statutory regimes[318] or self-generated promises of privacy. Hence, banks should be required to institute a policy of challenging non-mandatory NSLs or at least engaging in critical case-by-case review to determine whether NSLs should be challenged.

B. When Do Depositors Have a Right Against Banks Where Banks Fail to Exercise Their Full Rights Against the Government?

As demonstrated above, the FISA request process appears to involve less judicial oversight in practice than the text of section 215 might suggest. The revised FISA statute does not indicate upon what grounds a request will be struck down if challenged. Reasoning by analogy to the subpoena context, FISA requests will presumably be denied upon review when they fail to meet the minimal standard of showing that the records are sought for a foreign intelligence investigation.[319] Although courts have almost unanimously held that subpoenas are considered

317. *Id.* at 15–16. Note that Congress remained cautious of giving the FBI too much discretion in extending this grant of authority to issue NSLs with mandatory compliance. For example, the House Committee "carefully considered whether to grant the FBI mandatory access to financial records for foreign counterintelligence purposes upon a determination that there are specific and articulable facts giving reason to believe that an individual is or may be a foreign power or an agent of a foreign power" but rejected the "or may be" language as "provid[ing] an unwarranted degree of latitude." *Id.* at 17.

318. *See supra* Part III.B (detailing relevant statutory schemes).

319. Complaint for Declaratory & Injunctive Relief at 6–7, Muslim Comty. Ass'n of Ann Arbour v. Ashcroft, 459 F. Supp. 2d 592 (E.D. Mich. 2006) (No. 03–CV–72913–DT), *available at* http:// fl1.findlaw.com/news.findlaw.com/hdocs/docs/aclu/mcaa2ash73003cmp.pdf (Testimony of former Attorney General John Ashcroft).

compulsion by law,[320] and bank-customer privacy agreements typically allow for disclosure under such circumstances,[321] FISA requests are distinct from traditional subpoenas because customers are not notified and cannot object.

Furthermore, banks are bound not merely by the bare text of these privacy agreements, but also by their construction as contracts of adhesion.[322] Because provisions enumerating the circumstances under which a bank may disclose customer information are neither negotiable nor salient, there is little reason to believe that customers actually understand or accept these terms.[323] These contracts merit greater deference when they conform to publicly determined standards.[324] In this case, the Reauthorized Patriot Act evinces that Congress espouses a policy permitting banks to challenge FISA requests.[325] Given this development, courts should not be strong-armed by banks unilaterally limiting their obligations to customers through contracts of adhesion. Rather, courts should make their own determination as to whether the contracts are in line with congressional intent before honoring them.

In considering the customer expectations of privacy as reflected in the guiding principles behind legislative acts like the RFPA, judicial decisions similar to *Brex* and *Peterson*, and the very privacy policies distributed by banks themselves, a court may well conclude that banks should not yield to a FISA request without due consideration of the nature and basis of the request. This is even more apparent in the case of an NSL, which is not subjected to pre-enforcement judicial review and hence should not be considered compulsion by law.[326] Finally, non-mandatory NSLs are by definition not compulsory in nature.[327] When the issuing agency requests records on an admittedly optional basis, courts should be reluctant to hold that banks may comply pro

320. *See supra* Part III.C.2.b (explaining the necessary release of customer information under compulsion by law).

321. *See supra* Part III.C.3.c (discussing the vulnerabilities of adhesion contracts).

322. Rakoff, *supra* note 215, at 1176–80; *see generally supra* Part III.C.3 (examining bank contracts as contracts of adhesion).

323. Korobkin, *supra* note 222, at 1233.

324. Slawson, *supra* note 225, at 536.

325. 50 U.S.C.A. § 1861(f)(2)(A)(i) (West Supp. 2007); 18 U.S.C.A. § 3511(a) (West Supp. 2007).

326. *See supra* Part II.B (explaining how to obtain an NSL).

327. *See supra* Part II.C (discussing components of non-mandatory NSLs).

forma despite the promises in their relationships with their customers.[328]

C. Existing Challenges to Law Enforcement Inquiries for Financial Records

All of the federal privacy-promoting statutes contain exceptions that allow customer records to be disclosed without customer notice when the financial institution is served with formal process of law.[329] These exceptions are written narrowly and interpreted as such by the courts.[330] Although courts have not typically imposed liability on banks for disclosing records in response to a subpoena, they have sometimes imposed penalties on banks for complying with less formal processes.[331] These cases typically surface because bank customers have standing under the RFPA when banks divulge information despite the failure of the requesting authority to comply with the Act's procedural requirements.[332] For example, the instance of a bank responding to an oral request by law enforcement officials was held to violate the RFPA because the bank was not permitted to disclose information except in the case of customer authorization, subpoena, warrant, or formal written request.[333] In investigations concerning national security, however, customers cannot be notified that their

328. *E.g.*, Neece v. IRS, 922 F.2d 573, 577–78 (10th Cir. 1990) ("The provisions of the RFPA provide an elaborate mechanism to protect a taxpayer's privacy rights in records kept by third parties. We must protect this mechanism.").

329. *E.g.*, 15 U.S.C.A. § 6802(e)(8) (2000 & West Supp. 2007) (providing exceptions under which disclosure of nonpublic personal information is allowed).

330. *See supra* Part III.B (examing the relevant statutory schemes); John H. Derrick, *Rights and Remedies of Financial Institution Customer in Relation to Subpoena Duces Tecum Exception to General Prohibitions of State Right to Financial Privacy Statute*, 43 A.L.R. 4th 1157, 1158–59 (1986) ("In recognition of the fact that there are instances in which the state has a legitimate interest in obtaining such customer records, the [federal] statutes uniformly provide for an exception allowing disclosure without the consent of the customer under the authority of a subpoena duces tecum issued to the financial institution.").

331. *E.g.*, *Neece*, 922 F.2d at 576 (holding that a financial institution that is bound by the RFPA requires disclosure because it chooses to voluntarily allow the IRS to examine the financial records of one of its customers).

332. 12 U.S.C. § 3410(a) (2000) ("Within ten days of service or within fourteen days of mailing of a subpena [sic], summons, or formal written request, a customer may file a motion to quash an administrative summons or judicial subpena [sic], or an application to enjoin a Government authority from obtaining financial records pursuant to a formal written request, with copies served upon the Government authority.").

333. Anderson v. La Junta State Bank, 115 F.3d 756, 758 (10th Cir. 1997) (citing the narrow exceptions to 12 U.S.C. § 3402); *see also Neece*, 922 F.2d at 575 ("12 U.S.C. § 3402 of the RFPA specifies the only means by which federal agencies can obtain an individual's records in the possession of third-party record keepers such as financial institutions.").

records have been subpoenaed. Hence, they must rely on banks to vindicate their rights.

Customers have standing to object when banks disclose records of their own volition, without formal process by the requesting authority.[334] In less extreme cases, customers may also challenge disclosures that are not closely tailored to the issued subpoena. For example, a Maryland state court held that a customer could seek judicial relief from unauthorized disclosure of his financial records that were produced in a different time and place than specified in the subpoena.[335] Banks also have standing to bring a motion to quash a subpoena that directs them to release customer records.[336]

While customers do not have standing under the RFPA or other federal statutes to move for suppression of evidence obtained from unauthorized or unlawful disclosures,[337] they may have standing under state statutes. Courts in Colorado have reasoned that because bank customers maintained a reasonable expectation of privacy in their financial records, they had standing under the state Constitution to challenge a subpoena issued to the bank.[338] Courts in New Hampshire granted bank customers litigating for breach of privacy not only standing but also remedies, holding that suppression of records is an appropriate remedy when those records are obtained in violation of a state financial privacy statute.[339] State courts in Utah and Arizona have

334. *Neece*, 922 F.2d at 577–78. In response to the Bank Secrecy Act of 1970, customers complained that the recordkeeping requirements "undercut a depositor's right to effectively challenge a third-party summons." Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 51 (1974). The United States Supreme Court held that this scheme "works no injury on his bank" but withheld judgment on whether compulsion by subpoena of these records would give rise to depositor claims. *Id.* at 51.

335. Bond v. Slavin, 851 A.2d 598, 608 (Md. Ct. Spec. App. 2004) (holding that subpoenaed records should not have been delivered to the plaintiff's wife, instead of the court, without a hearing because "[t]he custodian cannot—without obtaining the permission of the person(s) whose financial records have been subpoenaed—produce those records at a different place on a different date"). While reaffirming that banks are compelled to release the requested records when presented with formal process, these courts have held that the disclosure is only permissible if it precisely conforms to the request.

336. Lincoln Bank & Trust Co. v. Okla. Tax Comm'n, 827 P.2d 1314, 1317 (Okla. 1992).

337. *E.g.*, *In re* Special Investigation No. 242, 452 A.2d 1319, 1322 (Md. Ct. Spec. App. 1982) (holding that the customer did not have standing to challenge a subpoena that was not directed at him, but rather at the bank to which he had voluntarily disclosed infomation).

338. Charnes v. DiGiacomo, 612 P.2d 1117, 1120 (Colo. 1980) (citing COLO. CONST. art. II, § 7).

339. *See* State v. Sheedy, 474 A.2d 1042, 1043 (N.H. 1984) ("[T]he suppression of any evidence obtained in violation of the Privacy Act is an appropriate remedy to vindicate the purpose behind the legislature's passage of the Privacy Act."); *see also* State v. Flynn, 464 A.2d 268, 274 (N.H. 1983) ("Therefore, we hold that the defendant has standing to challenge any

heard customer challenges and similarly granted motions to suppress financial records obtained through unlawful subpoenas on state constitutional grounds.[340] In Illinois, a bank customer was granted standing to challenge a subpoena of her financial records because she had a right of privacy in her financial records under the Illinois Constitution.[341] The Illinois court found that the most appropriate means of balancing the personal interest in privacy against the public interest in effective investigations was to use the validity of the subpoena as the test.[342]

The newly created ability of banks to raise objections to FISA requests is drafted in the Reauthorized Patriot Act as a privilege.[343] However, there is precedent for the argument that this privilege may become a duty under certain circumstances.[344] For example, a person seeking to compel inspection or production of records from the Federal Reserve Bank must file a written request with the Bank's general counsel before enforcing a subpoena.[345] More generally, courts in many jurisdictions have agreed that banks have standing to challenge

evidence obtained directly or indirectly from a violation of his privacy rights . . . . [I]nformation wrongly obtained from the defendant's accounts . . . may be suppressed.").

340. State v. Thompson, 810 P.2d 415, 419 (Utah 1991) ("Exclusion of illegally obtained evidence is a necessary consequence of police violations of article I, section 14.") (quoting State v. Larocco, 794 P.2d 460, 472 (Utah 1990)); *see also* State v. Bolt, 689 P.2d 519, 524 (Ariz. 1984) (holding the same based on a parallel provision in the Arizona state constitution).

341. ILL. CONST. art. I, § 6 ("The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or interceptions of communications by eavesdropping devices or other means."); People v. Jackson, 452 N.E.2d 85, 88–89 (Ill. App. Ct. 1983) ("In reliance upon this express proscription against invasion of privacy in Illinois and influenced by the Commentary which suggests that this protection should be broadly applied, we are led to conclude that the Illinois State Constitution offers protection for the reasonable expectation of privacy which our citizens have in their bank records."); *see also* 205 ILL. COMP. STAT. 5/48.1 (2006) (providing state statutory right to privacy and notice).

342. *Jackson*, 452 N.E.2d at 90 (holding that although plaintiff's right to privacy as guaranteed by the state constitution gave her standing to challenge the subpoena, the validity of the subpoena outweighed her privacy interests); *see also* Rycroft v. Gaddy, 314 S.E.2d 39, 42, 44 (S.C. Ct. App. 1984) (holding that a bank did not need to "look beyond the face of a valid subpoena" before complying by disclosing a customer's records).

343. 50 U.S.C.A. § 1861(f)(2)(A)(i) (West Supp. 2007) ("A person receiving a production order may challenge the legality of that order by filing a petition with the pool established by section 1803(e)(1) of this title.").

344. *See generally* Fed. Deposit Ins. Corp. v. Flagship Auto Ctr., 2005 U.S. Dist. LEXIS 9468, at *3 (N.D. Ohio May 13, 2005), *amended by* 2006 U.S. Dist. LEXIS 67876 (N.D. Ohio Sept. 21, 2006) (denying defendant's motion to compel documents from the Federal Reserve Bank).

345. *Id.* at 17 (finding that the written request must show that the need for confidential information outweighs the need to maintain confidentiality).

subpoenas on behalf of their customers.[346] These challenges to law enforcement inquiries in other contexts have set the stage for banks to use their newfound power to respect financial privacy in the face of national security investigations.

Although some courts have resisted banks who argued that their privacy policies prohibited them from abiding by subpoenas, these challenges have typically been struck down in cases where the privacy policies exempted the exact conduct being litigated.[347] In one such case, Bank of America had posted a privacy policy on its website indicating: "If we receive a subpoena or similar legal process demanding release of any information about you, we will generally attempt to notify you (unless we believe we are prohibited from doing so). Except as required by law . . . we do not share information with other parties, including government agencies."[348] Bank of America then received a subpoena requesting the production of customer records and prohibiting disclosure of the request to any third party.[349] The bank challenged the subpoena on the grounds that compliance would violate customers' Fourth Amendment right to privacy.[350] However, the Kansas state court held that "the right to privacy statement . . . does not create a privacy expectation in situations such as this where the agency is empowered to conduct an investigation in private."[351] The court classified the subpoena as "fall[ing] into the category excepted by Bank of America's recognition that it may be prohibited from notifying customers of the subpoena."[352] Hence, the court was not promulgating a blanket rule that privacy agreements could not be used to expand privacy protections, but rather implied that the privacy agreement in question as written did not determinatively expand confidentiality into

346. *See* Lincoln Bank & Trust Co. v. Okla. Tax Comm'n, 827 P.2d 1314, 1323 (Okla. 1992) (allowing a bank to bring suit for an injunction to enjoin the Oklahoma Tax Commission's administrative process for the inspection of financial records).

347. *E.g.*, Brant v. Bank of Am., 31 P.3d 952, 954 (Kan. 2001) (holding that despite the bank's privacy policy, the state securities commisioner, under his power to conduct private investigations, could prohibit the bank from disclosing to customers that a subpoena had been issued).

348. *Id.*

349. *Id.*

350. *Id.*

351. *Id*. at 960. *But see Brant*, 31 P.3d at 962 (Knudson, J., dissenting) ("Although I concede a bank customer in Kansas has no constitutional expectation of privacy in his or her bank records, most customers surely believe their banker will notify them if some government agency is snooping around in their records and accounts. I do not believe the legislature intended to negate that entirely rational and understandable expectation by the banking public.").

352. *Id*. at 959.

the circumstances of the case.[353] Similarly, the Supreme Judicial Court of Maine held that when presented with a formal request for records by the IRS, a bank was not obliged to delay compliance.[354] However, this holding was based not only on concerns about burdening the bank but also on the paucity of clear contractual language dictating how the bank should act in face of a subpoena.[355]

Generally, the person whose records are compelled by the subpoena is also the direct recipient of the subpoena and has an opportunity to challenge it by filing a motion to quash.[356] However, in the case of a bank subpoena sealed with a nondisclosure requirement, the subject of the subpoena is not in a position to request a judicial hearing by filing a motion to quash. "[T]herefore, a subpoena does not afford the person most affected the necessary opportunity to participate in compliance and insure accountability."[357] Under these circumstances, banks should rise to the occasion and defend their customers' privacy as Congress has authorized. Although they may choose to honor this obligation under the present contractual regime, financial institutions may also exercise their rights through contractual promises to engage in substantive review and challenge requests when appropriate.

V. CONTRACTING TO REQUIRE CHALLENGES TO REQUESTS FOR FINANCIAL RECORDS

Since Congress has given banks the statutory authorization to challenge FISA requests, customers may contractually obligate banks to take on this role. The Reauthorized Patriot Act has empowered banks but only created uncertainty for customers, who have no way to predict whether a bank would challenge requests for their records and under what circumstances.[358] The possibility that one's financial records may be disclosed in response to a government inquiry is more disconcerting to some customers than others. As one commentator has noted in

353. However, the court does generally come out in favor of allowing private investigations. *Id.* at 956 ("A target given notice of every subpoena issued to third parties would be able to discourage the recipients from complying.") (quoting and relying heavily on SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 750–51 (1984)).

354. Rush v. Maine, 387 A.2d 1127, 1128 (Me. 1978).

355. *Id.*

356. FED. R. CIV. P. 45(c)(3)(A).

357. Schulhofer, *supra* note 84, at 545.

358. *See* Steven A. Bibas, *A Contractual Approach to Data Privacy*, 17 HARV. J. L. & PUB. POL'Y 591, 609 (1994) ("[F]lexibility produces uncertainty for private parties. In the hands of the contracting parties, however, flexibility allows people to control their lives and efficiently tailor the law to meet their needs.").

considering personal valuations of financial privacy, the "golden mean" is "a solution tailored to individual preferences and values."[359]

Perhaps the least controversial version of such a contract would be a promise on the part of the bank to engage in some internal review or consultation to determine whether the request is lawfully authorized. If the bank determines that the FISA request is not lawful because it fails to meet the requirements of section 215, the bank would then be required to challenge it: a bank cannot be "compelled" to disclose information by an unlawful request.[360] While banks cannot be held liable by statute for disclosing records in response to a subpoena, they may be held liable on contractual grounds for failing to take the appropriate procedural precautions permitted by the statute and expected by customers.[361]

This final Part will describe the terms that a bank-customer agreement ensuring such challenges to disclosure might take. Since contracts that wholly bar reporting information to law enforcement authorities have been found void against public policy, this Article suggests that contracts incorporate a procedural hook requiring banks to challenge. This type of contract should not violate public policy norms because the Reauthorized Patriot Act authorizes exactly this kind of challenge to law enforcement inquiries.

A. Contractual Terms Requiring Banks to Challenge Law Enforcement Inquiries

As discussed in the preceding Part, privacy agreements as currently drafted may obligate banks to challenge some law enforcement inquiries in light of duties accrued from statutory protections or the banking tradition of confidentiality.[362] However, the tenuous nature of these financial privacy protections provides, at best, questionable assurance of privacy for customers.[363] In light of the recent procedural nod to

359. *Id.* at 593 ("Many people fear the loss of their privacy in a computerized 'Naked Society.' Others, however, are less concerned about the need for privacy and may be unwilling to sacrifice the benefits generated by the information economy."); *see also* Jonathan P. Graham, Note, *Privacy, Computers & the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395, 1424 (1986–1987) ("[T]he inflexible nature of an across-the-board statutory remedy might render the remedy inadequate to deal with the fluid nature of the information economy.").

360. *See* State v. Thompson, 810 P.2d 415, 418 (Utah. 1991).

361. 50 U.S.C.A. § 1861(e) (West 2003) ("A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production.").

362. *See supra* Part III (discussing privacy rights of depositors).

363. *See* Edgar & Walczak, *supra* note 289, at 22 (providing statistics which imply that ex ante judicial review is merely a rubber stamp).

financial privacy embedded in the Reauthorized Patriot Act, banks and their customers should be permitted to contract for more meaningful assurance that requests for financial records by law enforcement authorities will be challenged.[364] This could be structured as an absolute promise to challenge all requests, to challenge a particular kind of request (e.g., NSLs but not FISA requests), or more flexibly, a pledge to create a policy of internal review that would examine each request to determine whether a challenge would be appropriate. For example, in deciding whether to object to an administrative subpoena, institutions should consider the overarching legitimacy of the request, particularly whether the issuing agency was authorized to issue the subpoena and whether the subpoena seeks information protected by federal or state constitutional or statutory rights. In addition, institutions can analyze the specifics of the request, such as whether the subpoena was timely and properly served, whether it described the solicited documents with enough particularity, and whether the requested production would be unduly burdensome.[365] Because Congress has already proclaimed that these challenges are not incompatible with law enforcement investigations,[366] financial institutions and their customers should be able to build this procedural hook into their contracts explicitly.

Because the bank-customer relationship is contractual in origin, the two parties are free to establish its terms and require the financial institution to take on more protective or fiduciary-like duties.[367] Courts have recognized that a bank "may be made subject to any legal agreement which the depositor and the bank may make concerning it, so long as it does not injuriously affect the rights of innocent third parties."[368] Accordingly, courts have enforced contracts providing for confidentiality beyond the default standard of disclosure in other contexts, even when the contractual provisions conflicted with public interest. For example, the Court of Appeals for the Ninth Circuit held

364. *See generally supra* note 3 and accompanying text (discussing modifications of the original Patriot Act, including a nod to financial privacy).

365. Pamela Davis, What to Do When the Government Calls: Advising Clients on Government Demands for Personal Information on Customers and Others, Speech at PLI Conference (June 2004).

366. *See generally* 50 U.S.C.A. § 1861(f) (West Supp. 2007) (explicitly authorizing banks to bring these challenges).

367. Teeling v. Ind. Nat'l Bank, 436 N.E.2d 855, 858 (Ind. Ct. App. 1982) ("[T]he relationship between a depositor and a bank is contractual in nature, and the parties are generally free to establish a fiduciary relationship between themselves by agreement.").

368. Sindlinger v. Dep't Fin. Inst., 199 N.E. 715, 723 (Ind. 1936) ("If there is no [bad faith] connected with the transaction, the character of the deposit, whether general or special, is to be determined from the contract between the depositor and the bank.").

that a doctor who entered into a voluntary confidential agreement with his patient "was not at liberty to breach his obligation even when he felt it was in the public's best interest to do so."[369] The court found the doctor's "cho[ice] to limit his ability to share information" dispositive in overriding the norms of disclosure.[370] In holding the doctor liable for breach of confidentiality, the court noted the public policy favoring "the free-flow of information in a truth-finding process" but found that an adhered party cannot voluntarily testify to protected information.[371]

The banking context is particularly ripe for such contracting for heightened privacy protection because legislation foreshadows and sanctions this development. The GLBA requires that financial institutions "provide a clear and conspicuous disclosure of the institution's privacy policies" to customers.[372] In drafting this requirement, Congress clearly assumed that different institutions would provide varying levels of protections; if only the baseline protections mandated by the GLBA and RFPA were permissible, then no institutional notice would be necessary. Along with promoting flexibility in contracts and variety in privacy policies, the GLBA champions individual customers determining the level of disclosure they are willing to permit. For example, the GLBA allows customers to opt out of the sharing of their information with unaffiliated third parties by requiring banks to provide specific notice of any proposed disclosures and a reasonable period of time for the opt-out to occur.[373] Once a customer opts out, "a financial institution must honor that opt-out direction as soon as is reasonably practicable after the opt-out is received."[374] This principle of self-determination—allowing customers to take charge of the flow of their personal information and to play a role in the decisions governing the dissemination of their records among

369. Patton v. Cox, 276 F.3d 493, 499 (9th Cir. 2002).

370. *Id.*

371. *Id.* at 497. *But see* McGrane v. Reader's Digest Ass'n., 822 F. Supp. 1044, 1046 (S.D.N.Y. 1993) (demonstrating that in other contexts, such as employee trade secret agreements, "[c]ourts are increasingly reluctant to enforce secrecy arrangements where matters of substantial concern to the public—as distinct from trade secrets or other legitimately confidential information—may be allowed").

372. 15 U.S.C. § 6803(a) (2002 & West Supp. 2007).

373. F.T.C., In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act, http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.pdf (last visited Sept. 7, 2007); *see also* Swire, *supra* note 70, at 1263 (describing the GLBA as succesful privacy legislation).

374. F.T.C., Division of Financial Practices, Gramm-Leach-Bliley Act: Privacy of Consumer Financial Information, http://www.ftc.gov/privacy/glbact/glboutline.htm (last visited Sept. 7, 2007).

an array of presented options—would translate well into the context of contracting for pre-enforcement challenges.

B. Public Policy

In general, contracts can impose heightened obligations on banks: "The relationship between a depositor and a bank is contractual in nature, and the parties are generally free to establish a fiduciary relationship between themselves by agreement."[375] Article 4 of the Uniform Commercial Code ("UCC" or "the Code") elaborates the contractual principles controlling the bank-customer relationship, which is governed by the provisions of the written agreement along with the reasonable expectations described in the UCC. In general, the provisions provided by the Code serve only as a default and can be varied by agreement.[376] The only requirements that cannot be circumvented by contract are "good faith, diligence, reasonableness, and care."[377] These unalterable principles may serve as guideposts in determining whether bank-customer agreements obligating the bank to assume greater confidentiality are valid.

Contracts requiring banks to challenge law enforcement inquiries before releasing customer information might brush up against public policy exclusions to contract enforceability. Doctrinally, a contractual term is deemed unenforceable on public policy grounds if it contradicts relevant legislation or if a balancing of interests substantially disfavors its enforcement.[378] In weighing public policy against enforcing a contract, courts consider "the strength of the policy as manifested in legislation or judicial decisions," and whether "refusing to enforce the contract will further the policy or prevent misconduct, especially if serious, deliberate, or directly linked to the contract."[379]

Agreements categorically preventing banks from disclosing customer information would probably not be enforceable. Contracts interfering with law enforcement have generally been held void against public policy.[380] Courts also hesitate to punish someone for exposing the

375. Teeling v. Ind. Nat'l Bank, 436 N.E.2d 855, 858 (Ind. Ct. App. 1982).

376. U.C.C. § 1–102 (2005).

377. U.C.C. § 1–102(3) (2005).

378. RESTATEMENT (SECOND) OF CONTRACTS § 178(1) (1981); Town of Newton v. Rumery, 480 U.S. 386, 392 (1987) ("[A] promise is unenforceable if the interest in its enforcement is outweighed in the circumstances by a public policy harmed by enforcement of the agreement.").

379. RESTATEMENT (SECOND) OF CONTRACTS § 178(3) (1981); RICHARD A. LORD, WILLISTON ON CONTRACTS § 12:2 (4th ed. 1990).

380. 17A C.J.S. CONTRACTS § 234, at 204 (1999) ("Agreements which tend to suppress legal investigation concerning criminal offenses . . . are illegal as against public policy . . . .").

wrongdoing of another. As a result, contracts preventing the disclosure of information that would reveal the perpetrator of a crime are seldom enforced.[381] Courts have formalized this public policy exception by making unenforceable those contracts which intend to defraud or deceive third parties.[382] Some state courts have broadened the traditional public policy exceptions by holding that contracts that have the effect of preventing illicit activity from being reported are unenforceable even absent the element of intent or knowledge.[383] These exceptions manifest the reluctance of courts to enforce contracts that might injure third parties, even if such consequences were not anticipated.[384] Using a consequentialist approach, courts have declined to hold parties liable for breaching a contract in order to disclose suspicious activity: "A party bound by contract to silence, but suspecting that its silence would permit a crime to go undetected, would be forced to choose between breaching the contract and hoping that an actual crime is eventually proven, or honoring the contract while a possible crime goes unnoticed."[385]

In an analogous context, courts have also voided settlement agreements that barred the reporting of crimes to relevant law enforcement agencies on public policy grounds.[386] Courts have even resisted enforcing settlement agreements that do not explicitly conflict with the letter of the law if they generally prevent the revelation of suspicious activity to authorities.[387] In refusing to uphold a settlement agreement that purportedly barred reporting crimes to German

381. *See generally* 6A ARTHUR LINTON CORBIN, CORBIN ON CONTRACTS § 1455; RESTATEMENT (FIRST) OF CONTRACTS § 577 (1932).

382. *E.g.*, Lachman v. Sperry-Sun Surveying Co., 457 F.2d 850, 852 (10th Cir. 1972) ("An agreement, the [purpose] of which is the commission of a civil wrong against a third person, is also illegal . . . ."); *see also* Branzburg v. Hayes, 408 U.S. 665, 696 (1980) ("[I]t is obvious that agreements to conceal information relevant to commission of crime have very little to recommend them from the standpoint of public policy.").

383. In *Lachman*, the contract at issue was not entered into with the intent or knowledge of potential deceit. However, the court cited the more extreme case of *Singer*, in which a contract exchanging a promissory note for a promise to conceal a crime was held unenforceable, to stand for the proposition that the state "has expressed a stronger interest in the punishment of wrongful behavior than in the strict enforcement of contracts when the two interests collide." *Lachman*, 457 F.2d at 853.

384. *Id.*; *see also* Singer Sewing Mach. Co. v. Escoe, 64 P.2d 855, 857 (Okl. 1937) (noting that to enforce such a contract would be contrary to public policy). *See generally* Wilshire Oil Co. v. Riffe, 409 F.2d 1277, 1284-85 (10th Cir. 1969) (discussing plaintiff's ability to bring suit in an antitrust case).

385. *Lachman*, 457 F.2d at 854.

386. Fomby-Denson v. Dep't of Army, 247 F.3d 1366, 1373 (Fed. Cir. 2001) (citing RESTATEMENT (SECOND) OF CONTRACTS, Intro. to ch. 8, topic 1, at 5 (1981)).

387. *Id.* at 1375.

authorities, the Federal Circuit acknowledged that "there is no federal statute, treaty, or constitutional requirement mandating the referrals to the German law enforcement authorities."[388] However, the court applied the general presumption against enforcing contracts preventing disclosure of crimes in voiding the agreement: "We nonetheless conclude that the public policy interest at stake, the reporting of possible crimes to the authorities, is one of the highest order and is indisputably 'well defined and dominant' in the jurisprudence of contract."[389]

However, in considering whether a contract is void as against public policy, it is important to remember that there are competing policies at stake.[390] Factors in favor of enforcing a contract despite a potential conflict with public policy include "(a) the parties' justified expectations, (b) any forfeiture that would result if enforcement were denied, and (c) any special public interest in the enforcement of the particular term."[391] In the case of bank customers, the first two factors are weighted toward enforcing privacy agreements. As Congress indicated in passing the RFPA, customers reasonably expect that the information they are required to convey to banks to participate in financial transactions will be kept as confidential as is legally permissible.[392] Furthermore, the forfeiture of financial privacy is an irreparable harm that would foreseeably result in the failure to enforce these contracts.

Some commentators have criticized relying on public policy alone to determine the validity of contracts as "inflexible in application, at odds with the Code language, and difficult to utilize in giving protection across the broad spectrum of contract relations."[393] Public policy and unconscionability are imprecise means of determining when a contract should be unenforceable on its terms. As an alternative, courts could look to the guideposts of the Uniform Commercial Code's few unalterable requirements, namely good faith.[394]

388. *Id.*

389. *Id.* (quoting W.R. Grace & Co. v. Local Union 759, 461 U.S. 757, 766 (1983)); *see also* Roberts v. United States, 445 U.S. 552, 557 (1980) (referencing the historic duty of citizens to report crimes).

390. Price v. Hartford Accident & Indemnity Co., 502 P.2d 522, 524 (Ariz. 1972) (balancing the competing policies of freedom of contract with punishment and retribution in determining that an insurance policy covering punitive damages was not void as against public policy).

391. RESTATEMENT (SECOND) OF CONTRACTS § 178 (1981).

392. H.R. REP. NO. 95–1383, *supra* note 93, at 28.

393. Symons, *supra* note 98, at 240.

394. U.C.C. §§ 1–304 (2007); U.C.C. § 1–210(b)(20) (2007) (defining good faith as "honesty in fact and the observance of reasonable commercial standards of fair dealing"); U.C.C. § 3–103

In addition, a holistic conception of public policy should be multi-dimensional; the policy against interfering with an investigation does not operate in a vacuum, but must instead be counterbalanced by policies promoting financial privacy and freedom of contract. There are strong public policy reasons for favoring financial privacy. Courts have invoked the public policy of respecting confidentiality in a multitude of contexts. For example, an Oregon state court held that an employee, despite the at-will nature of his employment, could not be fired for refusing to reveal confidential financial information, citing a public policy exception to the at-will rule.[395] In the trade secret context, confidentiality agreements are typically enforceable except in cases when "public policy or the employee's interest outweighs the interest of the employer."[396] In deciding whether to enforce these agreements, states evaluate restrictions based on the nature of the employer's interests that the restrictions are intended to protect, whether they are reasonably related to this interest, how narrowly they are tailored, their duration, and how reasonable they are from a public policy standpoint.[397] Since courts have developed and implemented multi-factorial tests to evaluate the validity of trade secret agreements, they should be able to similarly formulate an approach to analyzing which contracts requiring banks to challenge law enforcement inquiries on behalf of their customers are enforceable and under what circumstances.

Furthermore, unlike the contracts that have been found void as against public policy because they effectively bar reporting to law enforcement authorities, the type of contract proposed here would merely include a procedural hook—and one which was legislatively created at that—to the disclosure process.[398] Some courts have permitted conditional disclosure agreements in other contexts. For example, the Federal District Court for the District of Kansas upheld a settlement agreement that prevented the plaintiff from voluntarily

cmt. 4 (2007) (explaining that the good faith standard requires "fairness of conduct," not merely the exercise of due care).

395. Banaitis v. Mitsubishi Bank, 879 P.2d 1288, 1294 (Or. Ct. App. 1994) ("In short, there is no requirement . . . that a specific statute has been violated before we may conclude that a societal obligation or a public duty has been implicated. We must review all the relevant 'evidence' of a particular public policy, whether that be expressed in constitutional and statutory provisions or in the caselaw of this or other jurisdictions.").

396. Carol M. Bast, *At What Price Silence: Are Confidentiality Agreements Enforceable?*, 25 WM. MITCHELL L. REV 627, 635 (1999).

397. *Id.* at 641.

398. *But see* Equal Employment Opportunity Comm'n v. Astra, 94 F.3d 738, 744 (1st Cir. 1996) ("In performing that balancing here, we must weigh the impact of settlement provisions that effectively bar cooperation with the EEOC on the enforcement of Title VII . . .").

cooperating with the Equal Employment Opportunity Commission.[399] In holding that the agreement was not void as against public policy, the court found it persuasive that the provision did not prevent the plaintiff from testifying in response to a subpoena.[400] Similarly, in this case, the proposed bank agreements would not bar disclosure altogether, but would only apply congressionally-sanctioned safeguards to individual cases.

C. Economic Feasibility of Contracting for Confidentiality and Place

In Part V.B, this Article addressed the enforceability of contracts wherein banks would promise to challenge subpoenas on behalf of their customers. In this Part, I will discuss whether the economics of such a promise would be feasible given the added cost to the bank and customer willingness to pay for this assurance.

Although case-specific data on the costs of challenging FISA requests or NSLs are not publicly available, extrapolation from more easily attainable data indicate that the costs, particularly when spread across a large number of bank customers, would be negligible. In an analogous consideration of the costs of challenging requests for customer records, Congress was unconcerned about the price tag of the proposed reform: when libraries challenge FISA requests, the litigation costs for the library's side are funded by taxpayers who finance the library's operation.[401] In passing S.2271, "[a] bill to clarify that individuals who receive FISA orders can challenge nondisclosure requirements," Congress projected that there would be "[no] discernable cost" to taxpayers.[402]

When courts have awarded attorney's fees for time spent preparing a motion to quash a subpoena, they have usually found awards around $5000 to be reasonable.[403] To be generous, let us estimate that it would

399. Hoffman v. United Telecomm., 687 F. Supp. 1512, 1515 (D. Kan. 1988).

400. *See id.* ("[The] settlement agreement limiting the plaintiff's cooperation in culminating the twelve-year-old investigation is not void as against public policy.").

401. TheWeekInCongress.com, http://www.theweekincongress.com/Member/MAR06_FULL/S2271PATRIOTshMAR10.htm (last visited Sept. 7, 2007)

402. *Id.* ("S.2271, a bill to clarify that individuals who receive FISA orders can challenge nondisclosure requirements, that individuals who receive national security letters are not required to disclose the name of their attorney, that libraries are not wire or electronic service providers unless they provide specific services, and for other purposes.").

403. *E.g.*, *In re* Mullins, 87 F.3d 1372, 1377 (D.C. Cir. 1996) (holding that fees arising from a motion to quash were reasonable); Panico v. Panico, 2006 WL 3703399, at *3 (Ohio Ct. App. Dec. 14, 2006); Mot. to Quash and/or Limit Subpoena Duces Tecum at 13, *In re* N. Tex. Specialty Physicians, No. 9312 (F.T.C. Jan. 7, 2004), *available at* http://www.ftc.gov/os/adjpro/

cost a bank $10,000 in attorney hours to challenge any given request for customer records. In 2005, there were approximately 2000 FISA requests.[404] Only a fraction of these were for bank records, but to err on the side of overestimation, let us assume that one-half related to financial institutions. From these rough estimations, the total cost of defending against all of the FISA requests would be $10 million.

According to the 2000 census, there are 210 million Americans over the age of eighteen.[405] At least seventy-five percent of these individuals are estimated to have some form of a bank account.[406] Accordingly, there are more than 150 million bank customers across the country. Given the estimated $10 million aggregate cost of challenging FISA requests, requiring banks to file motions to quash these subpoenas would average out to less than seven cents per customer.

There is some possibility of adverse selection: customers whose behavior would make them more likely to be the target of government investigation may accordingly be more inclined to opt for the assurance that banks will challenge FISA requests on their behalf.[407] However, even if only the one percent of customers most likely to be investigated selected to contract to require banks to challenge requests for their records, the total cost to banks of following through on the contracts would average out to be $6.67 per customer. Given the gravity of concern for financial privacy evinced in surveys of the American public,[408] it seems almost certain that many customers would value this additional safeguard on their privacy enough to pay at least this amount for it.[409] Furthermore, the widespread concern for financial privacy

d9312/040107bcbsmotoquashorlimitsdt.pdf; Midwest Fin. Corp. v. Equity Holding Co., 12 P.3d 475, 476 (Okla. Civ. App. 2000) ("Midwest was entitled to an award of attorney fees and costs incurred in responding to the Motion to Quash. The amount of fees and costs awarded ($5,422.71) was determined at a subsequent hearing.").

404. Letter from William E. Moschella, Assistant Attorney General, to J. Dennis Hastert, Speaker, U.S. House of Representatives (Apr. 28, 2006), *available at* http://www.fas.org/irp/agency/doj/fisa/2005rept.html.

405. JULIE MEYER, AGE: 2000, CENSUS 2000 BRIEF (2001), http://www.census.gov/prod/2001pubs/c2kbr01–12.pdf.

406. Lawrence H. Summers, Secretary of the Treasury, Remarks to the Enterprise Foundation's Annual Enterprise Network Conference, Generating Economic Opportunity for All Americans (Oct. 13, 1999), http://www.ustreas.gov/press/releases/ls153.htm (estimating that "between ten and twenty percent of American households still do not have any type of transaction account").

407. For a general discussion of adverse selection, see KENNETH S. ABRAHAM, INSURANCE LAW & REGULATION 6–7 (4th ed. 2005).

408. *See generally* Thorsberg, *supra* note 191 (discussing PC World survey).

409. *See generally* Bibas, *supra* note 358 (discussing how prices account for individual subjective valuations and reflect consumer preferences).

suggests that these contracts would be quite popular with many bank customers, and the more people who opt into the system, the lower the cost per customer will be.

If twenty-five percent of bank customers are willing to pay a small premium to require banks to challenge governmental inquiries on their behalf, the price per customer will be only twenty-six cents under the numbers and assumptions above, even assuming perfect adverse selection. This suggests that even if the above analysis is off by an order of magnitude, the price per customer would be low enough to make the contracts to challenge requests for customer records economically attractive and feasible.

VI. CONCLUSION

The Reauthorized Patriot Act empowers banks to protect their customers from unwarranted government inquiries by challenging FISA requests and NSLs. Although the terms of the Act provide banks with an option rather than a directive, banks should be required to exercise their newly granted powers in light of the promises they foster in their contracts and privacy statements. These documents, which are drafted and promulgated by banks, include express guarantees of confidentiality and should be construed to conform to the standards established by other financial privacy regulation. Given the place of confidentiality in the bank-customer relationship as developed by tradition and codified in federal and state legislation, banks should not blindly comply with government requests for records when they are permitted to exercise discretion in challenging FISA requests and NSLs.

Along with the obligations accrued under the current contractual regime, financial institutions can offer their customers greater privacy protection through contracts that explicitly obligate the institution to review government inquiries and challenge them when appropriate. In light of the recent congressional authorization of bank challenges to subpoenas of customer records, these contracts should be enforceable as consistent with public policy. Furthermore, given the small number of FISA requests relative to the large number of bank customers, the average cost per customer spent to challenge requests will be minimal. If banks wish to pass this cost along to customers who desire greater privacy protection, many customers will be willing to pay a small premium for the assurance that banks will more closely guard their personal information.