

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

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 Paper 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.

I.	Introduction	3
II.	Reauthorized Patriot Act	4
A.	Access to records under Amendments to FISA	5
B.	National Security Letters	8
C.	Non-mandatory NSLs	12
III.	The rights of depositors in information conveyed to financial institutions...14	
A.	Limited constitutional protections	15
B.	Extensive statutory schemes	18
1.	Right to Financial Privacy Act.....	19
2.	Gramm-Leach-Bliley Act	21
3.	State constitutional & statutory protections.....	23
C.	Contractual obligations of Banks.....	27
1.	Implied duty of confidentiality	27
a.	<i>The Bank-Customer Relationship</i>	27
b.	<i>Implied in contract</i>	31
2.	Explicit duties created by contractual language.....	35
a.	<i>Bank-customer agreements using permissive language</i>	37
b.	<i>Bank-customer agreements using restrictive language</i>	40
3.	Interpreting bank-customer agreements as contracts of adhesion	41
a.	<i>A Realistic Approach to Contracts of Adhesion</i>	42
b.	<i>Contracts of Adhesion as Private Lawmaking Meriting Judicial Scrutiny</i>	43
c.	<i>Particular Vulnerabilities of Contracts of Adhesion</i>	45
4.	Banks as private enterprise drafted into law enforcement by the state.....	48
IV.	Opportunities & obligations to challenge law enforcement inquiries.....51	
A.	Type of Law Enforcement Inquiry	53
1.	FISA Section 215 Requests	53
a.	<i>FISA Section 215 requests lack the ex ante procedural safeguard of warrants</i>	53
b.	<i>FISA Section 215 requests lack the ex post procedural safeguards of subpoenas</i>	56
2.	National Security Letters lack even the procedural protections of FISA requests ...	57
V.	Contracting to require challenges	62
A.	Terms?.....	63
B.	Existing challenges to law enforcement inquiries for financial records	66
C.	Public policy	70
VI.	Conclusion	76
	Appendix I: Market?	77

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 of the USA PATRIOT (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act of 2001 (hereinafter “Patriot Act of 2001” or “original Patriot Act”) was a small nod to financial privacy – a seeming check on the government’s power to obtain bank records without providing customers with notice or 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 will channel an era of enlarged customer privacy rights wholly depends on whether financial institutions will seize this opportunity to defend their customers’ records from intrusive government searches.

In this paper, I argue that this 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. Instead, the banks are confronted with exogenous sources of obligations that should inform their decision of whether to exercise this newly granted option of challenging law enforcement inquiries.

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

² Access to certain business records for foreign intelligence and international terrorism investigations, 50 U.S.C. § 1861(f)(2)(A)(i) (2006) (“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.”).

Although Supreme Court precedent indicates that customers enjoy only limited constitutional protection for privacy rights in financial information voluntarily conveyed to banks,³ a patchwork of federal statutory schemes speak to the importance of protecting financial information from unwarranted distribution.⁴ These federal rights are thickened by state constitutional and statutory protections.⁵ Furthermore, customers are endowed with contractual rights from the arrangements they enter into with the financial institutions to which they reveal private and sensitive information. These rights are embedded both in 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.⁶

In addition, I propose that banks and customers could explicitly contract to require banks to challenge law enforcement inquiries including subpoenas through clear duty-creating contractual language. I will propose feasible terms and explore the costs of following through on this obligation given the frequency of law enforcement inquiries and costs of raising petitions. Finally, I will consider whether there would be market demand for these additional privacy protections.

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.”⁷ Hence, Congress

³ See *infra* Sec. III.A.

⁴ See *infra* Sec. III.B.

⁵ See *infra* Subsec. III.B.3.

⁶ See *infra* Sec. III.C.

⁷ Viet D. Dinh & Wendy J. Keefer, *FISA & the PATRIOT Act: A Look Back & A Look Forward*, 35 GEO. L.J. ANN. REV. CRIM. PROC. iii, iv (2006); Charles Doyle, *USA Patriot Act: Provisions That Expire on December 31, 2005*, CRS Report for Congress (Jan. 2, 2004) (“Thereafter, the authority remains in effect only as it relates to

reconsidered much of the Act in drafting the Reauthorized Patriot Act. This Paper will focus solely on amendments to the original Patriot Act which implicated financial privacy in the investigative context.

A. Access to records under Amendments to FISA

As discussed above, the Reauthorized Patriot Act permits banks to challenge government requests for customer records. The statutory authorization for this newly conferred power comes from amendments to the Foreign Intelligence Surveillance Act (FISA), which gives the Federal Bureau of Investigation the power to issue confidential requests for financial records. Notably, Congress originally passed FISA in 1978 to bring greater Congressional oversight to counterterrorism operations. The Act, which reflected a concern that the Federal Bureau of Investigation (“FBI”), Central Investigative Agency (“CIA”), and Department of Defense (“DoD”) had abused their powers during the preceding decades, constituted a departure from the independence that agencies charged with protecting national security had originally enjoyed.⁸ In particular, FISA set boundaries on the use of electronic surveillance and subjected counterintelligence activities to judicial supervision. Under the FISA framework, FBI agents were permitted to conduct electronic searches and physical searches only after using information gathered by less intrusive techniques to satisfy the probable cause standard.⁹

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

foreign intelligence investigations begun before sunset or to offenses or potential offenses begun or occurring before that date.”).

⁸ Michael J. Woods, *Counterintelligence and Access to Transactional Records: A Practical History of the USA PATRIOT Act Section 215*, 1 J. NATIONAL SEC. L. & POL’Y 37, 40 (2005). (“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.”).

⁹ *Id.* (e.g., interviews, publicly available information and “surveillance in areas where no reasonable expectation of privacy exists”).

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." To address this concern, FISA created "a 'wall,' built of legal and policy requirements and reinforced by culture, that separated counter-intelligence officers from criminal investigators."¹⁰

This "wall" lasted until 2001, when it was dismantled by the Patriot Act of 2001. The Patriot Act amended FISA to allow the FBI to request individual financial records in the course of antiterrorism investigations and prohibited financial institutions from notifying their customers of any such requests.¹¹ This provision was among the most contentious extensions of federal law enforcement authority in the original Patriot Act. As Woods, speculates, "Perhaps no provision of the Act has generated more controversy than § 215, which authorizes the FBI to seek a court order compelling the production of 'any tangible things' relevant to certain counterintelligence and counterterrorism investigations."¹²

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.¹³ In reviewing the application, the judge must determine whether the application meets the statutory criteria, namely a factual showing of reasonable grounds, compliance with so-called

¹⁰ *Id.*

¹¹ 50 U.S.C. § 1861(a) (2006); 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.").

¹² Woods, *supra* note 8, at 37.

¹³ In reviewing a request for records under § 1861(a), judges use the criteria of 50 USC § 1803(a) (2006).

minimization procedures, and general lawfulness.¹⁴ If the judge concludes that the application satisfies these requirements, the judge shall enter an ex parte order approving the release of tangible things.¹⁵ The production order imposes a duty of nondisclosure on the party who is 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.¹⁶

Tucked into the Reauthorized Patriot Act is a provision empowering the institution from which records are solicited to challenge the production order:

The provision also expressly provides for a judicial review process that authorizes a specified pool of FISA court judges to review a 215 order that has been challenged. The provision requires high-level approval, and specific congressional reporting, of requests for certain sensitive categories of records, such as library, bookstore, tax return, firearms sales, educational, and medical records.¹⁷

While providing financial and other record-keeping institutions with this power to challenge subpoenas, the Reauthorized Patriot Act does not explicitly require these empowered institutions to exercise this option. On the contrary, the Act pronounces: “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.”¹⁸ 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

¹⁴ 50 U.S.C. § 1861(f)(2)(B), (C)(i) (2006) (clarifying the standard of judicial review as very narrow); Conference Report accompanying H.R. 3199, at 91 (Dec. 8, 2005), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_reports&docid=f:hr333.109.pdf (discussing section 106).

¹⁵ 50 U.S.C. § 1861(c)(1).

¹⁶ 50 U.S.C. § 1861(d)(1)(A), (B).

¹⁷ Conference Report accompanying H.R. 3199, *supra* note 14, at 91 (discussing section 106); § 1861(f)(2)(A)(i) (“The person receiving the production order may challenge its legality by filing a petition with the pool of designated district judges established by § 1803(e)(1).”).

¹⁸ 50 U.S.C. § 1861(e) (2006).

obligations and expectations preceding the 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 produce records by “certif[y]ing 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.”¹⁹ Congress granted agencies charged with protecting national security the power to issue NSLs to allow counterintelligence agents to obtain transactional information about investigative suspects.²⁰ When Congress first permitted these agencies to issue NSLs, it abstained from requiring the recipients of the letters to comply. Until 1978, it was left to the discretion of the institution whether to release the requested records on a case by case basis. In 1978, Congress passed the Right to Financial Privacy Act, which mandated that financial institutions comply with NSL requests for records. However, the RFPA only made compliance mandatory for the narrow set of record requests “where there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is or may be a foreign power or an agent of a foreign power.”²¹ In 1993, this requirement was reduced to “a connection with a suspected intelligence officer or suspected

¹⁹ 12 U.S.C. § 3414(a)(5)(A) (2006).

²⁰ Woods, *supra* note 8, 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,” e.g., records of bank accounts and money transfers).

²¹ S. Rep. No. 99-307, at 19 (1986).

terrorist or other indication of spying.”²² The 2001 Patriot Act promulgated an even more lenient standard, requiring only “relevance to an investigation of international terrorism or clandestine intelligence activities.”²³

In contrast to the FISA requests described above in Section II.A, the NSL issuance process involves few procedural safeguards to balance individual privacy against competing governmental interests. In a recent journalistic investigation uncovering the widespread use of the letters, Eric Lichtblau reported in the New York Times that “[a]s an investigative tool, the letters present relatively few hurdles; they can be authorized by supervisors rather than a court.”²⁴ 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. Lichtblau 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.”²⁵

Financial institutions are granted an opportunity to 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.²⁶ In

²² Dinh, *supra* note 7, at xx (citing 18 USC § 2709(b) (2000 & Supp. III 2003)).

²³ *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.”).

²⁴ Eric Lichtblau & Mark Mazzetti, *Military Expands Intelligence Role in US*, N.Y. TIMES, Jan. 14, 2007, available at <http://www.nytimes.com/2007/01/14/washington/14spy.html?ex=1169874000&en=118fa651b736ef03&ei=5070>; Rosen, *supra* note 23 (“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.”).

²⁵ Lichtblau, *supra* note 24.

²⁶ Judicial review of requests for information, 18 U.S.C. § 3511 (2006).

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.”²⁷ 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. 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 conclusive unless the court finds that it was made in bad faith.²⁸ 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. If the entity fails to obey the order, it may be held liable for contempt of court.²⁹

The availability of pre-enforcement judicial review of NSLs is essential to the constitutionality of the process. 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 the subpoena actually complies with the Fourth Amendment’s demands.”³⁰ An administrative subpoena regime would not be constitutional if judicial review was not available “prior to suffering penalties for refusing to comply.”³¹ In 2004, the federal district court for the

²⁷ Conference Report accompanying H.R. 3199, *supra* note 14, at 95 (explaining that the court may modify or set aside the nondisclosure requirement only if it ascertains 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.”).

²⁸ 12 U.S.C. § 3414(b)(2) (2006).

²⁹ 18 U.S.C. § 3511(c) (2006).

³⁰ *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 495 (S.D.N.Y. 2004). 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 7, at xxix.

³¹ *Id.*

Southern District of New York, in a decision upheld by 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.³² The ISPs argued that non-disclosure provision effectively prevented them from accessing the courts, because they would need to divulge the receipt of an NSL in order to litigate. 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.”³³ Courts have similarly rejected law enforcement processes compelling libraries to disclose borrower records without permitting pre-enforcement challenges.³⁴ As discussed above, the amended NSL provision in the Reauthorized Patriot Act allows recipients of the letters to challenge their issuance.³⁵ 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.³⁶

³² *Doe v. Gonzales*, 449 F.3d 415 (2d Cir. 2006) (holding 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 *Gonzales v. Doe II*, 386 F. Supp. 2d 66 (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) in holding that the recipient had demonstrated irreparable harm from the suppression of speech).

³³ *Doe v. Ashcroft*, 334 F. Supp. 2d at 505 (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”).

³⁴ *Doe v. Gonzales*, Opinion in Chambers (Oct. 7, 2005) (Ginsberg, J.), 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 (2d Cir. 2006)); compare Jay M. Zitter, *Constitutionality of National Security Letters Issued Pursuant to 18 USCA § 2709*, 2006 ALR Fed. 2d 3 (noting that the NSLs held unconstitutional in the internet service provider and library contexts are different than those issued to financial institutions).

³⁵ *Doe v. Gonzales*, 449 F.3d 415 (2d Cir. 2006).

³⁶ *Id.* at 419 (also vacating and remanding the First Amendment portion of *Doe v. Ashcroft* in response to the legislative changes).

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 § 215.³⁷ 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.³⁸ Rather, if the recipient of the letter does not comply, the government must approach a federal court for enforcement.³⁹ This suggests that Congress intended the NSL process to confer only limited authority to government agencies and wished to give courts a role in balancing law enforcement power with personal liberties.

C. Non-mandatory NSLs

In addition to the national security letters authorized by the Patriot Act, the U.S. military and the CIA have begun issuing “non-mandatory” national security letters as an extension of their domestic intelligence-gathering operations. The letters are mostly issued in connection with military or criminal investigations. However, the military and CIA not only lack the explicit statutory authority to issue NSLs granted to the FBI, but, as a former U.S. Deputy Assistant Secretary of State for International Law Enforcement notes, “[n]otably Congress has previously refused to provide these agencies with the authority to subpoena such documents, on the basis that the FBI already had this authority and that it was a bad idea to get the CIA and Defense Department to engage in domestic spying.”⁴⁰ In addition, as Elizabeth Parker, a former

³⁷ H.R. Rep. No. 107-236 (Part I), at 61. Compare *Endicott Johnson Corp. v. Perkins*, 317 U.S. 501, 509 (providing that the court must enforce an administrative subpoena unless it is “plainly . . . irrelevant to any lawful purpose of the agency”).

³⁸ Woods points out the distinction between 21 USC § 876(c), which provides for judicial enforcement of administrative subpoenas, and 12 USC § 3414(a)(5), which fails to provide for judicial enforcement of NSLs. Woods, *supra* note 8, at 61; see also Beryl A. Howell, *Surveillance Powers in the USA PATRIOT Act: How Scary Are They?*, 76 PA. BAR. ASSOC. Q. 12, 18 (2005).

³⁹ *Doe v. Ashcroft*, 334 F.2d 471 (S.D.N.Y. 2004).

⁴⁰ Jonathan Winer, CIA, Military Reveal Acquisition of Domestic Bank Records (Jan. 14, 2007), <http://www.counterterrorismblog.org/2007/01/> (“Given that the FBI already had this authority and has been using it

general counsel at both the National Security Agency and the CIA, has observed, these 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.”⁴¹ In general, courts have also reasoned that government surveillance in domestic affairs is entitled to greater constitutional protection than in the foreign intelligence context.⁴² Despite their questionable validity, officials estimate that thousands of these letters have been disseminated in the past few years.⁴³

Although these requests are admittedly non-mandatory (in contrast to FISA requests or NSLs issued by the FBI), journalistic investigations have revealed that “[b]anks, credit card companies and other financial institutions receiving the letters usually have turned over documents voluntarily, allowing investigators to examine the financial assets and transactions of American military personnel and civilians.”⁴⁴ 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 the terrorists.⁴⁵ Such disclosure raises serious civil liberties issues: “[W]hen the person under investigation is an American the justification for

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 24 (“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.”)

⁴¹ Lichtblau, *supra* note 24 (quoting Elizabeth Parker).

⁴² *United States v. United States District Court*, 407 U.S. 297 (1972) (“Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch.”).

⁴³ Lichtblau, *supra* note 24.

⁴⁴ *Id.*

⁴⁵ 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.

doing this without the normal procedural protections of a law enforcement investigation is hard to understand.”⁴⁶

Congress has not granted the authority to issue mandatory NSLs to the CIA or military. 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 coupled granting the authority to issue mandatory NSLs with other limitations on the breadth of this authority. 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.”⁴⁷ Furthermore, that Congress has given the FBI the right to issue mandatory NSLs 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.⁴⁸

III. The 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.”⁴⁹ However, the Supreme Court

⁴⁶ Winer, *supra* note 40.

⁴⁷ *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 481 (S.D.N.Y. 2004) (emphasis in original) (citing S. Rep. No. 99-307, at 19-20).

⁴⁸ *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, 1274 (noting that the Privacy Act has effectively “succeeded in preventing the creation of the omnivorous, unified federal database”).

⁴⁹ 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,

has not interpreted the Fourth Amendment as protecting information voluntarily conveyed to a third party.⁵⁰ However, Congress passed several statutes heightening customer protections by restricting the circumstances under which banks can release financial information.⁵¹ 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.⁵²

A. Limited constitutional protections

The bare language of the Fourth Amendment – particularly its inclusion of “papers” – might be construed to protect 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.

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.⁵³ However, the Court reasoned that the Fourth Amendment required law enforcement agents to comply with the “procedure of antecedent justification” before engaging in searches and seizures.⁵⁴ In *Katz*, government agents electronically listened to and recorded the petitioner’s calls made from a telephone booth. The

supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”) (emphasis added).

⁵⁰ *E.g.*, *U.S. v. Miller*, 307 U.S. 174 (1939).

⁵¹ *E.g.*, Right to Financial Privacy Act, 12 U.S.C. § 3401 (1978).

⁵² *Suburban Trust Co. v. Waller*, 408 A.2d 758, 764 (Md. App. 1979).

⁵³ 389 U.S. 347, 351 (1967).

⁵⁴ *Katz*, 389 U.S. at 359.

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.⁵⁵ 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.⁵⁶ 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.⁵⁷ By doing so, *Katz* "underscored the crucial role that disclosed by nonpublic information plays in modern society."⁵⁸ The reasoning of the *Katz* decision left open the possibility that customer financial records might be protected under the Fourth Amendment.

However, in *Miller*, the Court closed this possibility by holding that the search and seizure of bank records does not violate the Fourth Amendment because "the depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."⁵⁹ 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."⁶⁰

⁵⁵ *Id.* at 356.

⁵⁶ *Id.* at 351.

⁵⁷ *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.").

⁵⁸ *Id.* at 1103.

⁵⁹ *United States v. Miller*, 425 U.S. 435, 443 (1976). *But see* Stephen J. Schulhofer, *The New World of Foreign Intelligence Surveillance*, 17 STAN. L. & POL'Y REV. 531, 546 ("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.").

⁶⁰ *Id.* (citing *United States v. White*, 401 U.S. 745, 751-52 (1971)). 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. Compare *Schonewies v. Dando*, 435 N.W.2d 666, 671 (Neb. 1989).

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.⁶¹ 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."⁶²

Although the *Miller* decision has effectively closed off constitutional avenues for seeking privacy protection for financial records, some lower courts have skirted around the Supreme Court's holding by carving out privacy protections in analogous cases. For example, in *United States v. Thomas*, the Sixth Circuit held that individuals retained a reasonable expectation in the contents of their safety deposit boxes even though the boxes ostensibly belonged to the bank.⁶³ However, when it comes to financial records per se, it appears that there is little constitutional ground on which to argue for the protection of customer privacy in financial records.⁶⁴

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 to be 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."⁶⁵ Some state courts have

⁶¹ *Miller*, 425 U.S. at 345.

⁶² 385 U.S. 293, 302 (1966).

⁶³ 878 F.2d 383 (6th Cir. 1989).

⁶⁴ *Cf. Whalen v. Roe*, 429 U.S. 602, 603-04 (1977) ("recognize[ing] that in some circumstances the duty to avoid unwarranted disclosure of data arguably has its roots in the Constitution.").

⁶⁵ *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 494.

also given weight to banks' own interest in privacy. In Louisiana, one bank claimed that releasing private consumer financial information without customer consent would not only violate the GLBA, but also cause an irreparable injury to the bank, which fear[ed] that it would "surely suffer injury to its business reputation when its customers learn that their private financial information was divulged to third parties without their consent."⁶⁶ The state court agreed: "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."⁶⁷ Hence, there may still be a few constitutional avenues available to require banks to challenge FISAs request or NSLs on purely constitutional grounds. However, this paper's argument will not take a solely constitutional route, as the rights of bank customers are thickened 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. Congress has been cognizant of its ability to expand privacy protections for personal information, noting in 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."⁶⁸ 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*

⁶⁶ *Union Planters Bank v. Gavel*, 2002 WL 975675, at *2 (E.D. La. May 9, 2002).

⁶⁷ *Id.* at *6. *See also California Bankers Association v. Schultz*, 416 US 21, 51 (1974) ("It is true that in a limited class of cases this Court has permitted a party who suffered an injury as a result of the operation of law to assert his rights even though the sanction of the law was borne by another.")

⁶⁸ H.R. Rep. No. 95-1383, at 28 (1978), *reprinted in* 1978 U.S.C.C.A.N. 9273, 9304.

decision.⁶⁹ In this section, I 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.

1. 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. 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.”⁷⁰ The accompanying House Report specifically described the RFPA as an expansion of privacy protections in reaction to *Miller*:

The title is a congressional response to the Supreme Court decision in *United States v. Miller* The Court did not acknowledge the sensitive nature of [financial] records, and instead decided that since the records are the “property” of the financial institution, the customer has no constitutionally recognizable privacy in them.⁷¹

The RFPA prohibits financial institutions from disclosing records without notifying affected customers,⁷² and requires customer consent absent a search warrant, judicial subpoena, or formal written request.⁷³ This enactment empowers customers to object when the bank is presented

⁶⁹ Schulhofer, *supra* note 59, 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.”).

⁷⁰ H.R. Rep. No. 95-1383, *supra* note 68, at 28; Edward L. Symons, *The Bank-Customer Relation*, 100 *Banking L.J.* 220, 237 (“In 1978, Congress expressed its determination that, contrary to the majority opinion in *Miller*, a bank customer has a reasonable expectation of privacy his financial dealings with a bank.”).

⁷¹ H.R. Rep. No. 95-1383, *supra* note 68, at 28.

⁷² 12 U.S.C. § 3409.

⁷³ 12 U.S.C. § 3404 (customer authorization); § 3406 (search warrant); § 3407 (subpoena); § 3408 (written request). When the government subpoenas a customer’s records, the government must also provide a copy of the subpoena to the customer and along with a notice specifying the nature of the inquiry, § 3407(2).

with an administrative summons or judicial subpoena by filing a motion to quash or applying to enjoin the soliciting government agency.⁷⁴ 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.⁷⁵

However, the RFPA exempts from its procedural requirements investigations related to national security, counterterrorism, or foreign intelligence.⁷⁶ 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.”⁷⁷ 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.⁷⁸ Rather, the Act tracked traditional law enforcement procedures which generally require that when the Government seeks financial records of bank customers as part of a law enforcement inquiry, it must use formal written request such as a subpoena that is reviewable in court or obtain a search warrant.⁷⁹ In addition, the original RFPA required customer notice unless an order delaying notice was issued by a judicial officer. These protections have been chipped away over time. The RFPA was amended in 1987 by the Intelligence Authorization Act “to grant the FBI authority to obtain a customer's

⁷⁴ Customer challenges, 12 U.S.C. § 3410(a).

⁷⁵ Civil penalties, 12 U.S.C. § 3417(a).

⁷⁶ 12 U.S.C. § 3414(a)(1).

⁷⁷ 12 U.S.C. § 3414(a)(3)(A).

⁷⁸ Right to Financial Privacy Act § 1114(a).

⁷⁹ Robert T. Palmer & A.T. Darin Palmer, *Complying with the Right to Financial Privacy Act of 1978*, 96 BANKING L.J. 196, 211 (1979)

or entity's records from a financial institution for counterintelligence purposes if . . . there are specific and articulable facts giving reasons to believe that the customer or entity is a foreign power or an agent of a foreign power.”⁸⁰ However, despite this change in the evidentiary standard, the RFPA still reflects the importance of financial privacy as reaffirmed by Congress.

2. Gramm-Leach-Bliley Act

On November 12, 1999, Congress passed the Gramm-Leach-Bliley Act (GLBA) to modernize the regulation of financial institutions.⁸¹ One component of this modernization package was a reinvigoration of the central tenet of financial privacy. The GLBA announced: “It is the policy of Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ nonpublic personal information.”⁸² 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. However, it also contains a judicial process exception, allowing the financial institution to disclose personal information “to comply with Federal, state or local laws . . . subpoena or summons . . . judicial process or government regulatory authorities . . . or other purposes as authorized by law.”⁸³ Unlike the RFPA, the GLBA is focused on administrative oversight rather than private rights enforcement:

Significantly, the 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

⁸⁰ H.R. Rep. No. 99-690(I), at 14 (1986), reprinted in 1986 U.S.C.C.A.N. 5327, 5341.

⁸¹ Gramm-Leach-Bliley Act (also known as the Financial Services Modernization Act of 1999), Pub.L. 106-102, 113 Stat. 1338 (Nov. 12, 1999).

⁸² 15 U.S.C. § 6801(a).

⁸³ 15 U.S.C. § 6802(e)(8); *see, e.g., Ex parte Mutual Savings Co.*, 899 So. 2d 986 (Ala. 2004) (holding that trial court could order disclosure of customer info during civil discovery as part of GLBA’s judicial-process exception).

than to remedy or resolve individual rights affected by specific infractions.⁸⁴

Although the GLBA does not grant any new rights to depositors in the face of law enforcement inquiries, its legislative history provides an interesting window into the intent of Congress 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. 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:

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.⁸⁵

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. In light of these rapid changes and lagging responses, Gramlich urged Congress to "strike the appropriate balance between these competing interests."⁸⁶ Congress responded with the GLBA, which improved the ability of customers to exercise control over the dissemination of information contained in their bank records.

⁸⁴ David W. Roderer, *Tentative Steps Toward Financial Privacy*, 4 N.C. BANKING INST. 209, 212-13 (2000); see also 15 U.S.C. § 6801 (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").

⁸⁵ Statement of Edward Gramlich, Member, Board of Governors, The Federal Reserve System, House Banking Subcommittee Hearing (July 21, 1999), at 129 (available at http://commdocs.house.gov/committees/bank/hba58308.000/hba58308_1.HTM); see also *Indiv. References Serv. Grp., Inc. v. FTC.*, 145 F. Supp. 2d 6, 18-20 (D. D.C. 2001) (providing an extensive discussion of legislative history of the GLBA).

⁸⁶ *Id.*

3. State constitutional & 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.”⁸⁷ 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.⁸⁸ For example, the Colorado Supreme Court noted: “*Miller* limits our application of the Fourth Amendment . . . but it does not determine the scope of protection provided to individuals in Colorado by the constitution of this state.”⁸⁹ As scholars have explained:

For a state court interpreting a state constitution, opinions of the United States Supreme Court are like opinions of sister state courts or lower federal courts. One would expect a state court to deal carefully with a Supreme Court opinion and to explain forthrightly why it found itself constrained to reason differently. But such a difference in reasoning should be no more alarming than the differences which impel one judge to dissent from another's opinion, one court to disagree with another, or the judges of any court to disagree with a precedent established by their predecessors.⁹⁰

Justice Brennan has encouraged state courts to rise to the challenge of guaranteeing their litigants the full panoply of protections arising under their state constitutions. He cautions: “[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

⁸⁷ *Cooper v. State of California*, 386 U.S. 58, 62 (1967).

⁸⁸ *People v. Jackson*, 452 N.E.2d 85, 88 (Ill. App. 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.”); *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.”).

⁸⁹ *Charnes v. DiGiacomo*, 612 P.2d 1117, 1120 (Colo. 1980).

⁹⁰ Falk, *The State Constitution: A More Than “Adequate” Nonfederal Ground*, 61 CALIF. L. REV. 273, 283-84 (1973) (“While neither binding in a constitutional sense nor precedential in a jurisprudential one, [Supreme Court opinions] are entitled to whatever weight their reasoning and intellectual persuasiveness warrant.”).

extending beyond those required by the Supreme Court's interpretation of federal law.”⁹¹ Indeed, Justice Brennan expresses concern that the dramatic expansion of constitutional rights during the 1960s may have deterred state courts from taking full advantage of state-level guarantees, arguing that state-created rights are becoming increasingly important as more recent Supreme Court decisions interpret constitutional guarantees of civil liberties more narrowly.⁹²

Many state courts have analyzed the right to privacy in bank records under *Katz* instead of *Miller*.⁹³ 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.”⁹⁴ 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.⁹⁵ In an analogous move, the Illinois state courts have reasoned:

Under *Katz*, the Fourth Amendment gives protection for an individual's reasonable expectation of privacy which is not bound by the location and present ownership of the records. Consequently, the right to privacy is not waived by placing these records in the hands of a bank. The individual can still legitimately expect that her financial records will not be subject to disclosure.⁹⁶

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: “[T]he bank customers’ right of privacy in bank records, a state constitutional right,

⁹¹ William J. Brennan, Jr., *State Constitutions & the Protection of Individual Rights*, 90 HARV. L. REV. 489, 491 (1977).

⁹² *Id.* (“The legal revolution which has brought federal law to the fore must not be allowed to inhibit the independent protective force of state law--for without it, the full realization of our liberties cannot be guaranteed.”).

⁹³ *E.g.*, *State v. Thompson*, 810 P.2d 415, 418 (Ut. 1991).

⁹⁴ *E.g.*, *Community v. DeJohn*, 403 A.2d 1283, 1289 (Pa. 1979).

⁹⁵ *Charnes*, 612 P.2d at 1120; *Burrows v. Superior Court of San Bernardino County*, 529 P.2d 590 (Cal. 1974) (relying on Art. I, sec. 13 of the California constitution).

⁹⁶ *People v. Jackson*, 452 N.E.2d 85, 88 (Ill. 1983) (citing *Burrows*).

yields to an investigation of the pari-mutuel industry, which, to be effective, must be conducted without notice.”⁹⁷ However, in so reasoning, the court recognized this case to be an exception to the general state constitutional protection of financial privacy.

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 a statutory scheme which its state courts have interpreted as imbuing banks with a duty of confidentiality. 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. 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.”⁹⁸

Maryland has a more explicit state regime protecting the rights of bank customers. The Maryland legislature was “[a]pparently disturbed by what it believed to be a trend, out of all scotch and notch, among banks and other fiduciary institutions to furnish information without compulsion to government agencies”⁹⁹ and sought to re-emphasize that “the confidential relationships between fiduciary institutions and their customers must be preserved and protected.”¹⁰⁰ In light of its statutory regime, Maryland state courts have interpreted the

⁹⁷ *Winfield v. Div. of Pari-Mutuel Wagering*, 477 So.2d 544 (Fla.1985).

⁹⁸ *Burford v. First Nat. Bank in Mansfield*, 557 So.2d 1147, 1151 (La. App. 1990).

⁹⁹ *Suburban Trust Co. v. Waller*, 408 A.2d 758, 764 (Md. App. 1979).

¹⁰⁰ Preamble to 1976 Md. Laws, ch. 252(a)(2).

circumstances under which these customer confidences can be breached very narrowly, limiting banks to disclosing customer information under lawful court order or with customer consent.¹⁰¹

We think that a bank depositor in this State has a right to expect that the bank will, to the extent permitted by law, treat as confidential, all information regarding his account and any transaction relating thereto. Accordingly, we hold that, 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.¹⁰²

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.¹⁰³ These requirements go beyond “minimum constitutional requirements for the issuance of a search warrant.”¹⁰⁴ When the state statutory requirements are not met, bank customers have standing to challenge any evidence obtained without procedural authorization.¹⁰⁵ Alabama has also enacted statutes which prohibit the disclosure of customer bank records except upon subpoena or court order.¹⁰⁶ These state enactments not only provide additional safeguards and courses of action for bank customers, but underscore the importance of financial privacy in society's collective consciousness.

¹⁰¹ *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” as “afford[ing] the Bank more protection than it was entitled to receive”). *Cf.* 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.” *Indiana National Bank v. Chapman*, 482 N.E.2d 474, 481 (Ind. App. 1985) (citing *Indiana Bell Telephone v. State*, 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.*

¹⁰² *Suburban*, 408 A.2d at 764.

¹⁰³ Obtaining Records by Search Warrant, N.H. Rev. Stat. Ann. § 359-C:9 (Supp. 1991); N.H. Rev. Stat. Ann. § 359-C:4, I (Supp.1981).

¹⁰⁴ *State v. Sheedy*, 474 A.2d 1042, 1044 (N.H. 1984) (citing Pt. 1, Art. 19 of the New Hampshire state constitution along with the Fourth Amendment to the U.S. Constitution).

¹⁰⁵ *Id.*; *State v. Flynn*, 464 A.2d 268, 274 (N.H. 1983) (discussed *infra* note 290).

¹⁰⁶ Comment to Disclosure of customer financial records, Ala. Code § 5-5A-43 (1980).

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 taken on roles as agents and fiduciaries, hence implicating the duties of confidentiality and loyalty.

1. Implied duty of confidentiality

a. *The Bank-Customer Relationship*

Under a classic debtor-creditor relationship, there is no expectation of privacy.¹⁰⁷ However, courts have hesitated to classify the bank and customer as merely a debtor and creditor.¹⁰⁸ Rather, judicial descriptions of the relationship operating within the broadly construed confines of the debtor-creditor model have thickened the classic conception by inferring a limited duty of privacy: “The 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.”¹⁰⁹ 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 customer’s records:

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 actual money deposited is concerned, that is true. But as to the records . . . there is an

¹⁰⁷ *Schoneweis v. Dando*, 435 N.W.2d 666 (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.

¹⁰⁸ E.g., *Frame v. Boatman’s Bank*, 824 S.W.2d 491, 495 (Mo. App. 1992); *Brex v. Smith*, 146 A. 34, 36 (N.J. 1929).

¹⁰⁹ *Frame*, 824 S.W.2d at 495.

implied obligation . . . on the bank to keep these from scrutiny until compelled by a court of competent jurisdiction to do otherwise.¹¹⁰

One reason for this distinction between deposited money and bank records is the high value placed on financial privacy. As courts in several jurisdictions have recognized: “Of all the rights of the citizen, few are of greater importance . . . but exemption of his private affairs, books and papers from the inspection and scrutiny of others.”¹¹¹

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 rules of agency.”¹¹² In so finding, the court cited a variety of cases across jurisdictions holding that banks must comply with their depositors’ orders.¹¹³ 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 customer’s agent for the purpose of disclosing information. From this characterization the court inferred that the duty of confidentiality which prohibits an agent from disclosing information to the principal's detriment applies with regard to banks disclosing customer information.¹¹⁴ An

¹¹⁰ *Brex*, 146 A. at 36.

¹¹¹ *In re Pacific RR Commission*, 32 F. 241, 250 (C.C.D. Cal. 1887); see also *Interstate Commerce Comm’n v. Brimson*, 154 U.S. 447, 479 (1894) (decrying law enforcement inquiries that resemble “fishing expeditions”).

¹¹² *Peterson v. Idaho First Nat’l Bank*, 367 P.2d 284, 289 (Id. 1961).

¹¹³ See, e.g., *Crawford v. West 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.”); *Dalamatinsko v. First Union Trust & Sav. Bank*, 268 Ill. App. 314 (1932). 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 “the 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. App. 1948) (holding that bank breached duty in paying 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 NW2d 861, 864 (Neb. 1955) (citing 9 CJS, Banks & Banking § 267, p. 546).

¹¹⁴ Blumstein & Pohly, *Confidentiality, Access & Certainty: Disclosure of Customer Bank Records*, 1982 ANN. REV. BANKING L. 101, 114.

agency relationship entails confidentiality: “An agent is subject to a duty to the principal not to use or to communicate information confidentially given to him by the principal or acquired by him.”¹¹⁵ 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.¹¹⁶ In a fiduciary relationship, the fiduciary “has a duty to act primarily for the benefit of another.”¹¹⁷ 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 will exercise its power over property deposited for its own benefit.”¹¹⁸ Although fiduciary relationships are creatures of contract and malleably turn on the reasonable expectations of the parties, most courts and scholars agree that “[t]he manifestations of the parties in most bank-customer relations do not give rise to reasonable expectations of a fiduciary relation.”¹¹⁹ 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

¹¹⁵ *Peterson*, 367 P.2d at 289 (quoting RESTATEMENT OF LAW OF AGENCY 2d, § 395).

¹¹⁶ “The 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. JR. 2D BANKS & FIN. INST. § 720. 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 (Fla. App. 1985) (“Where 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 National Bank*, 67 F. Supp. 616, 624 (S.D. Ala. 1946) (considering banks to be the fiduciaries of their depositors).

¹¹⁷ RESTATEMENT (SECOND) OF TRUSTS, §§ 2, 170, Comment a (1959).

¹¹⁸ Symons, *supra* note 70, at 232.

¹¹⁹ *Id.* at 231 (citing RESTATEMENT (SECOND) OF AGENCY § 1 Comment 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).

party to relax the care and vigilance it would ordinarily have exercised in dealing with a stranger.” Under such circumstances, “a bank may be held liable for breaching its duty of confidentiality in disclosing the financial condition of its customers and depositors.”¹²⁰ A fiduciary relationship may also “arise out of a relationship of confidence, trust, or superior knowledge or control.”¹²¹ 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.¹²²

Although customers do not benefit from the full protections of a fiduciary relationship, the incorporation of the concept of agency along with the special value placed on financial records have imputed some privacy protections into the bank-customer relationship: “Courts have recognized the special considerations inherent in the bank-depositor relationship and have not hesitated to find that a bank implicitly warrants to maintain, in strict confidence, information regarding its depositor’s affairs.”¹²³ In 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, strictly speaking, one composed of equals because of the inordinate power of the bank.” Given the “precarious position of the borrower and the relatively superior position of the bank,” courts have recognized “a counterbalancing special duty imposed on the part of the bank,” namely

¹²⁰ Edward J. Raymond, Bank’s liability, under state law, for disclosing financial information concerning depositor or customer, 81 ALR 4th 377 § 7 (discussing *Rubenstein v. South Denver Nat. Bank*, 762 P.2d 755 (Colo. App. 1988)).

¹²¹ *Broadway Nat’l Bank v. Barton-Russell Corp.*, 585 N.Y.S.2d 889, 945 (1992).

¹²² See *Gaunt v. Peoples Trust Bank*, 379 N.E.2d 495 (Ind. Ct. App. 1978); *Klein v. First Edina Nat’l Bank*, 196 N.W.2d 619 (Minn. 1978).

¹²³ *Suburban Trust Co. v. Waller*, 408 A.2d 758, 670 (Md. App. 1979) (holding that absent legal compulsion, bank could not reveal info to police) (followed by *Taylor v. Nationsbank*, 776 A.2d 645 (Md. 2001); *White v. Regions Bank*, 729 So.2d 856 (Ala. Civ. 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.

confidentiality.¹²⁴ Hence, while banks are not the fiduciaries of their depositors, they do not enjoy unbridled discretion with regard to customer records.

b. Implied in contract

Courts have recognized the implied contract as “a form of express contract wherein the elements of the contract are found in and determined from the relations of and the communications between the parties, rather than from a single clearly expressed written document.”¹²⁵ In contrast to cases in which 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.¹²⁶ 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.”¹²⁷

Courts have historically found confidentiality to be an implied term in bank-customer agreements. In 1924, the King’s Bench in England reasoned, in 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 term of a banker’s contract with

¹²⁴ *Djowharzadeh v. City National Bank*, 646 P.2d 616, 619-20 (Okla. 1982).

¹²⁵ *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, 423 (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.”).

¹²⁶ U.C.C. § 1-205(3) (“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.”).

¹²⁷ Statement of Edward Gramlich, *supra* note 85.

his customer that the bank shall not disclose the account.”¹²⁸ This notion was adopted by American banking law, which came to recognize “implied in the contract a certain duty of confidentiality.”¹²⁹ 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.”¹³⁰

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. As the Supreme Court of Idaho reasoned:

It is implicit in the contract of the bank with its customer or depositor that no information may be disclosed by the bank or its employees concerning the customer's or depositor's account, and that, unless authorized by law or by the customer or depositor, the bank must be held liable for breach of the implied contract.¹³¹

¹²⁸ *Tournier v. Nat'l Provincial & Union Bank*, 1 K.B. 461, 480 (1924); *see also* 10 AM.JUR.2D BANKS § 332 (“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, either express or implied . . . unless the banker is compelled to do so by order of a court.”).

¹²⁹ ZOLLMANN, BANKS & BANKING (Vol. 5) § 3413, pp. 379-80 (Depositors have a right of secrecy. A bank therefore is under an implied obligation to keep secret its records of accounts, deposits, and withdrawals.”); I.F.G. BAXTER, THE LAW OF BANKING 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 (Id. 1961); *Brex v. Smith*, 146 A. 34, 36 (N.J. 1929); *Suburban Trust Co. v. Waller*, 408 A.2d 758, 764 (Md. App. 1979).

¹³⁰ *United States v. First National 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 (1977) (“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.”).

¹³¹ *Peterson v. Idaho First Nat'l Bank*, 367 P.2d 284, 290 (Id. 1961).

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 and state or federal privacy statutes.¹³²

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 trusts the bank to hold his information as confidential and that the bank invites or accepts this trust, courts have noted that "banks present a constant invitation to intending borrowers, and thus subject themselves to whatever implication or obligation is to be drawn from fact."¹³³ 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."¹³⁴ 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."¹³⁵ In light of these expansive proclamations of financial privacy, "[b]oth Congress and the state legislatures have provided a statutory base to clarify some common reasonable expectations of bank customers."¹³⁶ Hence, most courts agree that at a minimum, "at least, a bank has an obligation to its customers not to disclose unnecessarily, promiscuously, or maliciously their financial

¹³² *Garfield v. NationsBank*, 776 A.2d 645 (Md. 2001) (holding that the bank which released its customer's records without consent or compulsion liable for breach of contract, privacy, and confidentiality but finding no statutory violations).

¹³³ *M.L. Stewart & Co. v. Marcus*, 207 N.Y.S. 685 (1924); *Dolton v. Capitol Fed. Sav. & Loan Ass'n*, 642 P.2d 21 (Colo. App. 1981).

¹³⁴ Privacy Statement, Bryant Bank (2005), <http://www.bryantbank.com/index.asp?page=951>.

¹³⁵ Privacy Policy, First Guaranty Bank (2006), <http://www.fgb.net/PrivacyPolicy.htm>.

¹³⁶ Symons, *supra* 70, at 244 ("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.").

condition.”¹³⁷ 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.¹³⁸

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 society without maintaining a bank account.”¹³⁹ Even the American Banking Association has espoused the position that banks “should, as a general policy, consider information concerning its customers [as] confidential, which it should not disclose to others without clear justification.”¹⁴⁰ Financial records are particularly sensitive because “[t]he totality of bank records provides a virtual biography.”¹⁴¹ When providing such extensive information to banks, customers expect that the information will be only be used internally.¹⁴² 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

¹³⁷ *Rubenstein v. S. Denver National Bank*, 762 P.2d 755 (Colo. App. 1988) (citing *State v. McCray*, 551 P.2d 1376 (Wash. App. 1976)).

¹³⁸ *O'Connor v. Ortega*, 480 U.S. 709, 715-17 (1987) (discussing whether an employer’s search of employee’s workplace is considered a violation of the employee’s Fourth Amendment rights).

¹³⁹ *Burrows v. Superior Court of San Bernardino Valley*, 529 P.2d 590, 596 (Cal. 1974); Schulhofer, *supra* note 59, 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.”).

¹⁴⁰ *Milohnoch v. First Nat’l Bank*, 224 So. 2d 759, 761 (Fla. App. 1969) (finding breach of implied contractual duty for disclosure to third parties); *compare* 12 C.F.R. § 309.1 (1988) (disclosure of information guidelines for the Federal Deposit Insurance Corporation).

¹⁴¹ *Burrows*, 529 P.2d at 596.

¹⁴² *See* Blumstein & Pohly, *supra* note 114, at 109-10.

not be seen as conduct which constitutes a waiver of an expectation of privacy.¹⁴³

Similarly, the Supreme Court of Pennsylvania held that borrowers and depositors have a “right to be secure against unreasonable searches and seizures” in “all papers which [they] supplied to the bank to facilitate the conduct of [their] financial affairs upon the reasonable assumption that the information would remain confidential.”¹⁴⁴

2. Explicit duties 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 as debtor-creditor or fiduciary, which are “nothing more than specialty contract relations—contract relations shaped by recurring special facts and circumstance . . . determined by the intentions of the parties’ manifested intent creates a middle-ground contract relation,” courts would be better off explicitly relying on contractual notions to define the relationship between the parties. Such deference to contracts would not only better reflect the parties’ intent but also encourage more precise contracting.¹⁴⁵

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

We recognize the customers’ 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

¹⁴³ *State v. Thompson*, 810 P.2d 415, 418 (Ut. 1991) (“Such a biography should not be subject to an unreasonable seizure by the State government.”); *People v. Jackson*, 452 N.E.2d at 89 (Ill. 1983).

¹⁴⁴ *Commonwealth v. DeJohn*, 403 A.2d 1283, 1290 (Pa. 1979).

¹⁴⁵ Edward L. Symons, *supra* note 70, at 225-26 (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.”).

assets is our customers' trust, therefore, confidentiality and safekeeping of customer information is a priority.¹⁴⁶

Such customer agreements invoke notions of privacy that closely track the conception of confidentiality espoused in *Brex*, *Burrows*, *Suburban*, and *Peterson*,¹⁴⁷ and shape the expectations of customers: “Although historically the adoption of such privacy policies or privacy principles may be done on a voluntary basis, it is important to recognize that the incorporation of such principles into customer agreements, or even the communication of such principles to individual customers, can create enforceable rights for customers.”¹⁴⁸ These privacy agreements also represent a change in expectations of privacy since *Miller* was decided thirty years ago: “Commercial enterprises and financial institutions today commonly allow customers to state a preference about how their personal information will be used, and they often market guarantees of privacy. From this, a customer now could reasonably conclude that he or she retained control over data entrusted to these third parties.”¹⁴⁹

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). A contemporaneous Harris poll also found that more Americans supported

¹⁴⁶ First Community Bank, N.A., and People's Community Bank, A Division of First Community Bank, N.A., Privacy Policy (May 24, 2005), https://www.fcbresource.com/privacy_statement.cfm.

¹⁴⁷ *Brex v. Smith*, 146 A. 34, 36 (N.J. 1929); *Burrows v. Superior Court of San Bernardino County*, 529 P.2d 590 (Cal. 1974); *Suburban Trust Co. v. Waller*, 408 A.2d 758, 764 (Md. App. 1979); *Peterson v. Idaho First Nat'l Bank*, 367 P.2d 284, 290 (Id. 1961).

¹⁴⁸ L. Richard Fischer, *Emerging Issues in the World of Financial Privacy*, Consumer Financial Services Litigation, PLI Order No. B0-00NC (Apr. 2000).

¹⁴⁹ Woods, *supra* note 8, 42-43 (however, Woods concludes that “*Miller* remains the law for now.”).

face-recognition technology to scan for suspected terrorists than closer monitoring of financial transactions.¹⁵⁰

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.”¹⁵¹ Similarly, Bank of America states: “We also may disclose . . . Customer Information to credit bureaus and similar organizations and when required or permitted by law.”¹⁵² The phrase “as permitted” has been interpreted narrowly by courts. When a bank 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. 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

¹⁵⁰ Frank Thorsberg, *PC World Poll Highlights Privacy Concerns*, PCWorld.com (Friday, October 5, 2001), <http://www.pcworld.com/article/id,64824-page,1/article.html>.

¹⁵¹ *E.g.*, Sovereign Bank Privacy Policy and Interactive Reporting & Initiation Services (IRIS) Account Security Overview (January 2007), <http://www.sovereignbank.com/corporate/downloads/cashmanagement/infereporting/irisprivacyandsecurity.pdf>; Privacy Statement, Bryant Bank, <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.”).

¹⁵² Bank of America Privacy Policy for Consumers 2007, http://www.bankofamerica.com/privacy/index.cfm?template=privacysecur_cnsmr; Chevy Chase Bank Privacy Pledge, <http://www.chevychasebank.com/htm/privacy.html> (“We do not disclose any non-public personal information about our customers to any other third parties, except as permitted or required by law.”); 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> (“You do not have to respond to this notice in any way because we share your information only as required or permitted by law.”).

conduct was not explicitly sanctioned by Virginia law.¹⁵³ This language has been interpreted in other contexts as “intended to limit the creditor’s discretion in disposing of the collateral and to apply the same law that governed the security agreements.”¹⁵⁴ Analogously, when an agreement allows one of the parties to “disclose confidential information . . . to a court . . . in furtherance of U.S. legal proceedings,” this language is 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.”¹⁵⁵

Other banks claim that they will not disclose customer information except “when authorized by law.” For example, Jackson State Bank notes in its privacy statement, “We 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.”¹⁵⁶ 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.”¹⁵⁷ This language has generally been interpreted in favor of disclosure, giving considerable deference to law enforcement authorities.¹⁵⁸ Under the GLBA, banks are authorized to disclose customer information:

[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

¹⁵³ *West v. Costen*, 558 F. Supp. 564 (W.D. Va. 1983).

¹⁵⁴ *United States v. Terrey*, 554 F.2d 685, 692 (5th Cir. 1977) (holding that United States Small Business Administration had a duty to dispose of property in commercially reasonable manner and that “as permitted” clause was intended as to limit discretion); *Peoples Bank of the Virgin Islands v. Figueroa*, 559 F.2d 914 (3d Cir. 1977) (holding that banks could not volunteer information or respond to unauthorized requests “without breaching duties of confidentiality and privacy in its dealings with its customers).

¹⁵⁵ *Interclaim Holdings, Ltd. v. Ness*, 2001 U.S. Dist. Lexis 17945, *25 (N.D. Ill. Oct. 29, 2001).

¹⁵⁶ The Jackson State Bank & Trust Policy on Customer Confidentiality and Privacy of Information, <http://www.jacksonstatebank.com/custserv/privacy.cfm>.

¹⁵⁷ 12 U.S.C. § 3407(1).

¹⁵⁸ *Irani v. United States*, 448 F.3d 507 (3d 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)).

government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law.¹⁵⁹

When the bank has received a subpoena or summons, courts generally find the bank to be “authorized” to comply even if the customer objects. Banks have been allowed to simply ignore customer opposition in complying with subpoenas: “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.”¹⁶⁰ Courts have allowed banks to disclose such information despite acknowledging the duty of confidentiality.¹⁶¹ In doing so, courts have ranked the duty of confidentiality as subordinate to the duty to comply with subpoenas and summons.¹⁶² 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.¹⁶³

¹⁵⁹ 15 U.S.C. § 6802(e)(8).

¹⁶⁰ *Chapman v. Solar*, 2006 U.S. Dist Lexis 68805, *8 (M.D. Fla. Sept. 8, 2006) (“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 (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 Federal Savings & Loan Assoc.*, 560 F. Supp. 245, 247 (N.D. Ill. 1983).

¹⁶¹ 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 (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); *Rush v. Maine Savings Bank*, 387 A.2d 1127 (Me. 1978); *Kansas Comm’n on Civil Rights v. Sears, Roebuck & Co.*, 532 P.2d 1263 (Kan. 1975) (upholding disclosure of credit information pursuant to administrative subpoena); *Rycroft v. Gaddy*, 314 S.E.2d 39 (S.C. App. 1984).

¹⁶² 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, 630 (1985).

¹⁶³ “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, United States Attorneys’ Tax Resource Manual 55B (Feb. 2007), http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title6/tax0055b.htm. *Contra* 50 U.S.C. § 1861(f) (2006) (allowing banks to challenge FISA requests for customer records); 18 U.S.C. § 5311 (2006) (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.¹⁶⁴ For example, the Alabama state courts have noted: "It is now well settled that 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."¹⁶⁵ Some banks have also contracted to abide to this narrow standard of disclosure.¹⁶⁶ Notably, a subpoena is generally considered compulsion.¹⁶⁷ 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.¹⁶⁸

If the recipient objects, the serving party may not inspect or copy any of the requested records unless the court which 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

¹⁶⁴ *Bond v. Slavin*, 157 Md. App. 340, 851 A.2d 598 (2004); *Suburban Trust Co. v. Waller*, 408 A.2d 758, 764 (Md. App. 1979); see also *Peoples Bank of the Virgin Islands v. Figueroa*, 559 F.2d 914 (3d Cir. 1977) (bank volunteering information breaches duty of confidentiality).

¹⁶⁵ *White v. Regions Bank*, 729 So. 2d 856 (Ala. Civ. App. 1998) (internal quotations omitted).

¹⁶⁶ E.g., Privacy Policy Disclosure, Iowa State Bank & Trust Company (September 2006), <http://www.isbt.com/privacy.php>.

¹⁶⁷ "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." Raymond, 81 ALR 4th § 10 (discussing *O'Coin v. Woonsocket Institution 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*, 424 S.E.2d 431, 435 (N.C. 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 438. Hence, courts often interpret the exceptions to these privacy agreements more broadly than the text of the provisions would suggest.

¹⁶⁸ FED. R. CIV. P. 45(c)(3)(A)(iii).

because a court could not compel production of these confidential and sensitive data.¹⁶⁹ Hence, this Paper's argument that subpoenaed entities may be required to object to a subpoena to preserve the confidentiality of a third party's information is not without legally sanctioned precedent. 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 section, banking contracts are contracts of adhesion which should be interpreted as privately drafted laws.

3. Interpreting bank-customer agreements as contracts of adhesion

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.¹⁷⁰ 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.¹⁷¹ Consolidating the factors into a simple litmus test, Arthur Leff defines contracts of adhesion as “that which would be a contract except that no bargaining power

¹⁶⁹ Fed. Deposit Insu. Corp., 2005 U.S. Dist LEXIS 9468 (N.D. Oh. May 13, 2005) (holding that a court could not compel production of “suspicious activity reports”) (citing FED. R. CIV. P. 45(c)(2)(B)).

¹⁷⁰ Todd D. Rakoff, *Contracts of Adhesion: An Essay in Reconstruction*, 96 HARV. L. REV. 1173, 1176-80 (1983).

¹⁷¹ *Burrows v. Superior Court of San Bernadino Valley*, 529 P.2d 590, 596 (Cal. 1974).

really shapes it.”¹⁷² Historically, contracts of adhesion have generally been upheld, except in cases where the terms or circumstances fall within the traditional exceptions to enforceability such as fraud, inducement, or unconscionability.¹⁷³ More recently, courts have expanded upon these historic exceptions by also refusing to hold the adhered party to such a contract “[w]here the other party has reason to believe that party manifesting the assent would not do so if he knew that the writing contained a particular term, the term is not part of the agreement.”¹⁷⁴

a. A Realistic Approach to Contracts of Adhesion

Traditional doctrine proposes that parties should be bound to contracts of adhesion: since the adherent had an opportunity to read, his agreement signifies assent to the terms.¹⁷⁵ 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 since the terms are not negotiable.¹⁷⁶ In reality, customers “are boundedly rational decisionmakers who will normally price only a limited number of product attributes as part of their purchase decision.” Drafters capitalize on this inherent limitation by supplementing the salient attributes of the contract with self-favoring

¹⁷² Arthur Leff, *Contract as Thing*, 19 AM. U. L. REV. 131 (1970); see also *Brex v. Smith*, 146 A. 34 (1929); *Burrows*, 529 P.2d at 595.

¹⁷³ *Id.*; see also Thomas H. Oehmke, Adhesion Contracts, 1 Commercial Arbitration § 9:1 (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.”).

¹⁷⁴ RESTATEMENT (SECOND) OF CONTRACTS § 211. 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”).

¹⁷⁵ *Lewis v. Great Western Railway*, 5 H. & N. 867, 157 Eng. Rep. 1427 (Ex. 1860); Rakoff, *supra* note 170, at 1185-87 (discussing and critiquing the historic approach); see also KARL LLEWELYN, THE COMMON LAW TRADITION 370 (1962) (arguing that blanket assent can be inferred from agreement because of the signor’s opportunity to read).

¹⁷⁶ Rakoff, *supra* note 170, at 1128.

terms.¹⁷⁷ Accounting for the predictably self-dealing behavior of the drafting party, Leff 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.”¹⁷⁸ 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.

b. Contracts of Adhesion as Private Lawmaking Meriting Judicial Scrutiny

Standard form contracts can be likened to privately made law because they “impos[e] officially enforceable duties or creat[e] or restrict[] officially enforceable rights.”¹⁷⁹ 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.¹⁸⁰ Whether contracts of adhesion conform to publicly determined standards is a helpful heuristic to figure out whether they should be enforced. As David Slawson has argued: “Conformity to standards also facilitates control because the standards to which we require conformity are those which

¹⁷⁷ Russell Korobkin, *Bounded Rationality, Standard Form Contracts, and Unconscionability*, 70 U. CHI. L. REV. 1203, 1203 (2003).

¹⁷⁸ Leff, *supra* note 172.

¹⁷⁹ W. David Slawson, *Standard Form Contracts & Democratic Control of Lawmaking Power*, 84 HARV. L. REV. 529, 530 (1971).

¹⁸⁰ See *Amalgamated Meat Cutters & Butcher Workmen of North America, AFL-CIO v. Connally*, 337 F. Supp. 737 (D. D.C. 1971) (holding that the statute did not breach the non-delegation doctrine NDD 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 Schechter 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).

bear on the factors we consider relevant.”¹⁸¹ 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, “Rather than holding the bank only to those obligations that it has freely assumed, as a matter of fixed public policy, Congress has imposed upon banks other obligations of confidentiality. These obligations have been imposed based on a legislatively determined sense of fairness and reasonableness established to protect expectations or perceived needs.”¹⁸² Judicial review is essential to determining whether individual contracting systems conform to such legislative standards. Although courts typically uphold contracts unless their provisions were egregious enough to be considered fraudulent, induced, or unconscionable,¹⁸³ courts should apply a more scrutinizing standard of review to contracts likened to private lawmaking. Slawson makes the case for a more critical approach to contracts of adhesion by noting 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.

Contracts are based on a meeting of the minds and embody the intentions of the contracting parties.¹⁸⁴ Hence, Slawson encourages courts to parse contractual provisions closely to discern which ones reflect shared intent: “[O]nly the expressions, or manifestations, of consent of the contracting parties should be called the contract and should be enforced, generally,

¹⁸¹ Slawson, *supra* note 179, at 536.

¹⁸² Symons, *supra* note 70, at 244 (1983).

¹⁸³ U.C.C. § 1-304 (“Every contract or duty within [the Uniform Commercial Code] imposes an obligation of good faith in its performance or enforcement.”); U.C.C. § 2-302 (“If the court as a matter of law finds the contract or any term of the contract to have been unconscionable at the time it was made, the court may refuse to enforce the contract . . .”).

¹⁸⁴ “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.” ROBERT E. SCOTT & JODY S. KRAUS, *CONTRACT LAW & THEORY* 676-77 (3d ed. 2002).

without question.”¹⁸⁵ In enforcing contracts, courts generally honor the reasonable expectations of the parties.¹⁸⁶ Courts should be particularly cognizant of what those expectations were at the time of contracting 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 Slawson recognizes: “Reasonable expectations are determined not by what the form recites but by the actual context in which the transaction is conducted.”¹⁸⁷

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 would 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.”¹⁸⁸ Of particular concern with regard to disclosure provisions is that “individuals might treat certain low-probability risks as if they were virtually non-existent” because “they are excessively confident in their likelihood of avoiding harm.” Furthermore, “people 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.”¹⁸⁹

¹⁸⁵ Slawson, *supra* note 179, at 541 (concluding that “[t]he standard form is not a contract”).

¹⁸⁶ *E.g.*, *Allen v. Prudential Property & Cas. Ins. Co.*, 839 P.2d 798, 801 (Ut. 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).

¹⁸⁷ Slawson, *supra* note 179, at 544.

¹⁸⁸ Rakoff, *supra* note 170, at 1255.

¹⁸⁹ Korobkin, *supra* note 177, at 1233. *Contra* Andrew Kull, *Mistake, Frustration & the Windfall Principle of Contract Remedies*, 43 HASTINGS L.J. 1 (1991) (courts may not be any more well-positioned to allocate risks of unexpected contingencies than the parties drafting the contracts).

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.¹⁹⁰

Knowing that customers lack the willingness and ability to evaluate contingent terms such as disclosure procedures, banks realize only a few terms will engage customer attention and need to be drafted in a favorable manner.¹⁹¹ 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 or because all competitors use the same clauses.”¹⁹² 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.¹⁹³ Instead of espousing a uniform presumption of enforceability or 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.”¹⁹⁴

A more draconian approach to contracts of adhesion than conditioning enforceability upon conformance to societal, democratically-developed standards is considering adhesive terms to be presumptively unenforceable. The two approaches are may often lead to a shared outcome

¹⁹⁰ *Compare What Price Privacy?*, 56 CONSUMER REPORTS 356 (May 1991, Issue 5) (“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.’”).

¹⁹¹ Korobkin, *supra* note 177.

¹⁹² Friedrich Kessler, *Contracts of Adhesion - Some Thoughts About Freedom of Contract*, 43 COLUM. L. REV. 629, 640 (1943).

¹⁹³ *Id.*

¹⁹⁴ *Id.* at 642.

since “[m]any of the terms in typical form documents are specifically designed to displace clear rules of law that would otherwise govern the transaction”¹⁹⁵ and such terms would not be upheld under a litmus test of conformance. This approach has been proposed by Rakoff, who questions judicial deference to adhesive contracts in light who their drafters are, noting that “business firms do not resemble the types of voluntary organizations to which the law gives great deference.”¹⁹⁶ 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.”¹⁹⁷ This suggests that judicial review, either under the historic deference to contracts of adhesion or even under the heightened scrutiny proposed by Slawson may be insufficient to efficiently protect customer expectations. 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.”¹⁹⁸

Critics of adhesive contracts 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. However, many see higher prices as preferable to misleading customers by enforcing contracts that do not conform to their expectations. As Rakoff infers, “If 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

¹⁹⁵ Rakoff, *supra* note 170, 1183.

¹⁹⁶ *Id.* at 1241 (arguing that considering standard-form contracts to be presumptively enforceable would not endanger freedom of contract among individuals).

¹⁹⁷ Korobkin, *supra* note 177, at 1249.

¹⁹⁸ Rakoff, *supra* note 170, at 1265.

leads adherents to focus exclusively on visible terms.”¹⁹⁹ This Paper will address customer willingness to pay a premium for greater protection of financial information in the Appendix.

4. Banks as private enterprise drafted into law enforcement by the state

As discussed in the section above, courts should approach terms in bank agreements allowing banks to disclose customer information to law enforcement authorities with greater scrutiny because customers may not have willingly and knowingly agreed to these terms. Even when these terms comply with the relevant federal laws requiring the collection and disclosure of customer information, question remain as to 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 not prefer to privatize its information collection schemes because society is often more skeptical of the motives of profit-maximizing private entities.²⁰⁰ 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.²⁰¹ 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 particularly

¹⁹⁹ *Id.*

²⁰⁰ Christopher D. Stone, *Corporate Vices & Corporate Virtues: Do Public/Private Distinctions Matter?*, 130 U. PA. L. REV. 1441, 1459 (“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.”).

²⁰¹ 50 U.S.C. § 1861(d).

cavalier about the risks involved in its behavior, having the unique capability to justify its actions as “in the public interest” despite the potentially adverse effects.²⁰²

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.²⁰³ The government is considered an agent subject to control by the public, unlike private organizations like 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 much greater public outcry than a government policy of secretly requesting the same information from banks rather than their customers.²⁰⁴ 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 farmed out to complicit private entities.²⁰⁵

Furthermore, non-compulsory NSLs are being issued by agencies which could not get access to these records through the usual avenues of inter-agency cooperation or congressional

²⁰² Stone, *supra* note 200, at 1459 (citing the Tuskegee study in which syphilis was “studied” instead of cured and the leukemia exposures from testing nuclear weapons); *see also California Bankers Association 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 the 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 not conscripted neutrals in transactions involving negotiable instruments, but parties to the instruments with a substantial stake in their continued availability and acceptance.”).

²⁰³ Stone, *supra* note 200, at 1467 (also noting that the public may be less keen on punishing government entities because the penalties would be drawn from taxpayers’ pockets).

²⁰⁴ For example, the government long kept its phone monitoring program under wraps. Government Monitoring About 200 Million Phone Calls, ABC News – Good Morning America (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. *Electronic Privacy Information Center v. Dep’t of Justice* (D.D.C. complaint filed Aug. 2, 2000), available at <http://www.epic.org/privacy/carnivore/complaint.pdf>; *FBI’s System to Covertly Search Email Raises Privacy, Legal Issues*, *Wall St. J.*, July 11, 2000.

²⁰⁵ Robert Schmul, *Government Accountability & External Watchdogs*, ISSUES OF DEMOCRACY (August 2000), <http://usinfo.state.gov/journals/itdhr/0800/ijde/schmuhl.htm>.

mandate.²⁰⁶ 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.²⁰⁷ However, the fact that the CIA and DoD could not get Congressional backing for their national security letters implies something about the political unwillingness of elected parties to support this scheme.²⁰⁸

By masking the gathering of information through nondisclosure requirements that prevent banks from notifying customers that their records have been requested, the government has largely evaded the heightened scrutiny courts apply to state action.²⁰⁹ It is possible that a strategic move to privatize information collection in order to avoid judicial inference of constitutional obligations would be ineffectual since the courts could easily look beyond the nominally private actor to discern the underlying state actor.²¹⁰ However, this veneer of private action can be quite effective since courts are, in practice, often reluctant to reclassify private actors as essentially public.²¹¹

However, judicial control is particularly essential in the financial privacy context because the public is ill-equipped to effectively monitor government activity.²¹² Courts are the only

²⁰⁶ See *infra* Sec. II.C.

²⁰⁷ J.Q. Wilson & P. Rachal, *Can the Government Regulate Itself?*, THE PUBLIC INTEREST 3-4 (Winter 1997); Stone, *supra* note 200, at 1501 (“[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.”).

²⁰⁸ See *infra* Sec. II.C.

²⁰⁹ Stone, *supra* note 200, 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 (1980)..

²¹⁰ For § 1983 actions, private actors are sometimes considered to be engaging in state action when they act in concert with government officials. E.g., *Pennzoil v. Texaco*, 481 U.S. 1 (1987) (holding that a creditor invoking the state’s judgment-enforcement mechanism may be considered a state actor); *West v. Atkins*, 487 U.S. 42 (1988) (holding that a private physician who treated prison inmates in a state facility was engaging in state action).

²¹¹ For example, the Supreme Court refused to find state action in the case of a “private” school which operated almost solely to provide specialized teaching services under a government contract. *Rendell-Baker v. Kohn*, 457 U.S. 830 (1982). Consequently, the Court denied the teachers’ section 1983 civil rights claims because the it failed to find that the school officials were acting under color of state law. *Id.* at 836 (denying plaintiffs’ First, Fourth, and Fourteenth Amendment claims).

²¹² Stone, *supra* note 200, 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

entities informed of FISA requests and NSLs, and even then only in the minority of cases where banks bring challenges. Hence, judicial remedies must supplement the political processes that generally serve as a check on state actors. The Supreme Court considered 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.”²¹³ However, in that case regarding the constitutionality of the 1970 Bank Secrecy Act, the Court held that since the banks were merely maintaining records and only disclosing transactions to the government when faced with a subpoena, there was no illegal search or seizure.²¹⁴

IV. Opportunities & 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 type of relationship, and the jurisdiction.

Bank Secrecy Act and declined to find violations of the First, Fourth, Fifth, or Fourteenth Amendments. *E.g.*, *California Bankers Association v. Schultz*, 416 U.S. 21 (1974).

²¹³ *Id.* at 22.

²¹⁴ *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.”).

As discussed above, neither the FISA nor the NSL statute, in giving banks the power to object to law enforcement inquiries, requires the exercise of this newly granted authority.²¹⁵ However, customers expect that banks will guard their information and protect their privacy.²¹⁶ 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 banks draft for their customers to sign.²¹⁷ 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.²¹⁸

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 these 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.²¹⁹ Given the circumstances surrounding their origin, the precise language of bank-customer agreements should not be entitled to deference unless they conform to democratically-determined standards,²²⁰ namely the respect for financial privacy reflected by Congressional enactments such as the RFPFA, GLBA

²¹⁵ 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).

²¹⁶ *Infra* Subsec. III.C.1.a.

²¹⁷ *Infra* Subsec. III.C.2.

²¹⁸ *Infra* notes 173-75.

²¹⁹ Slawson, *supra* note 179, at 544.

²²⁰ Symons, *supra* note 70, at 244.

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 in under compulsion by law.²²¹ Courts have generally considered subpoenas to be compulsion, valuing bank compliance with law enforcement over customer confidentiality.²²² In other contexts, courts tend to be deferential to subpoenas when ruling on a motion to quash.²²³ However, I will argue in this section that the unique circumstances surrounding FISA requests for records and NSLs warrant greater judicial scrutiny.

1. FISA Section 215 Requests

a. FISA Section 215 requests lack the ex ante procedural safeguard of warrants

At first brush, effectuating a request for documents under Section 215 looks similar to obtaining a search warrant because both require judicial approval.²²⁴ 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.²²⁵ Rather than the showing of probable cause required to typically obtain a search warrant, the applicant need only show that the records are

²²¹ Privacy Policy Disclosure, Iowa State Bank & Trust Company, <http://www.isbt.com/privacy.php> (September 2006); The Jackson State Bank & Trust Policy On Customer Confidentiality and Privacy of Information, <http://www.jacksonstatebank.com/custserv/privacy.cfm>; Bank of America Privacy Policy for Consumers 2007, http://www.bankofamerica.com/privacy/index.cfm?template=privacysecur_cnsmr.

²²² *E.g.*, *White v. Regions Bank*, 729 So. 2d 856 (Ala. Civ. App. 1998).

²²³ *E.g.*, *Rush v. Maine*, 387 A.2d 1127 (Me. 1978).

²²⁴ *Infra* Sec. II.B.

²²⁵ Schulhofer, *supra* note 59, at 533.

sought for a foreign intelligence, clandestine, or international terrorism investigation.²²⁶ 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.”²²⁷

Furthermore, the agency is not required to show any special need for secrecy which requesting a clandestine search.²²⁸ “Thus, although FISA requires a court order, the judge’s role is far more limited than in domestic law enforcement situations.”²²⁹ These emaciated judicial protections are coupled with greater flexibility in investigative procedures than is typically permitted in conventional criminal investigations. Perhaps most notably, FISA authorizes clandestine search tactics which prevent the suspect from being notified. Even if the suspect is eventually prosecuted, the defense attorney is not usually permitted to review the associated surveillance documents. In addition, FISA searches may be authorized for broader timelines with less judicial supervision than in conventional investigations.²³⁰

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. 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.²³¹ As

²²⁶ Former Attorney General John Ashcroft has testified 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.” Testimony to the House Judiciary Committee (June 5, 2003).

²²⁷ *Muslim Community Association of Ann Arbor v. Ashcroft*, Complaint at 6, <http://f11.findlaw.com/news.findlaw.com/hdocs/docs/aclu/mcaa2ash73003cmp.pdf>.

²²⁸ Schulhofer, *supra* note 59, at 544.

²²⁹ *Id.* at 533.

²³⁰ *Id.* at 534.

²³¹ 18 U.S.C. 2520(g), 2707(g) (imposing civil liability for any willful use or unauthorized disclosure of information); 18 U.S.C. 2712 (creating a cause of action against the United States for victims of

commentators have concluded: “In all of these respects, the FISA regime offers far less accountability and a greatly enhanced risk of abuse.”²³²

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 approved. Before 2001, the FISA Court received about 750 applications per year and had never rejected a single one.²³³ In 2003, the FISC reviewed 1724 applications and denied only four. These numbers have led notable civil liberties groups to refer to the FISC as a rubber stamp.²³⁴ 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. In the 2001 Patriot Act, both of these requirements were dropped and replaced only by a good-faith standard.²³⁵ 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.²³⁶

willful violations of the FISA requirements relating to surveillance or physical searches). *But see* Schulhofer, *supra* note 59, 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.”).

²³² Schulhofer, *supra* note 59, at 538; *see also* Patrick Leahy, Charles Grasse & Arlen Specter, FBI Oversight in the 107th Congress by the Senate Judiciary Committee: FISA Implementation Failures, An Interim Report (Feb. 2003), *available at* (Grassley.senate.gov/releases/2003/p03r02-25c.pdf).

²³³ Foreign Intelligence Surveillance Act Orders 1979-2005, Electronic Privacy Information Center (May 2, 2006), www.epic.org/privacy/wiretap/stats/fisa_stats.html.

²³⁴ Timothy Edgar & Witold Walczak, *We Can Be Both Safe & Free: How the PATRIOT Act Threatens Civil Liberties*, 76 PA. BAR. ASSOC. 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.”).

²³⁵ Schulhofer, *supra* note 59, at 548-49 (“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.”)

²³⁶ § 1861(b)(2) & (c)(1).

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. However, 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.²³⁷ 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.”²³⁸ The recipient may file a motion to quash and receive a hearing in front of a judge. Although the requirements which must be met for a subpoena to be upheld as valid are minimal, “judicial oversight, even in this highly diluted form, does act as a check on unrestricted official snooping, and it provides the subpoena recipient an important guarantee of accountability.”²³⁹ Furthermore, judicial oversight may be particularly influential in the arena of financial privacy, since 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.²⁴⁰

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. Unless banks challenge these subpoenas, “they eliminate any opportunity to seek a judicial inquiry into the reason for an investigative demand and the significance of the information sought” along with “virtually any possibility of public

²³⁷ FED. R. CIV. P. 45(c)(3)(A).

²³⁸ Schulhofer, *supra* note 59, at 545.

²³⁹ *Id.*

²⁴⁰ Jack W. Campbell, *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 (10th Cir. 1974). Compare FED. R. CIV. P. 69 (allowing compulsion of financial records to enforce a judgment).

criticism.”²⁴¹ This is particularly disturbing since judicial review has been called “the most common and important civil liberties protection.”²⁴²

2. National Security Letters lack even the procedural protections of FISA requests

The NSL process lacks the 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.²⁴³ Courts only enter the process if the recipient of the letter petitions to have the letter modified or set aside.²⁴⁴ 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 national security letters.

Banks should take it upon themselves to challenge national security letters 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 exception should not be interpreted to include NSLs.²⁴⁵ 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.²⁴⁶ NSLs are not backed by a

²⁴¹ Schulhofer, *supra* note 59, at 554.

²⁴² Edgar & Walczak, *supra* note 234, at 22.

²⁴³ 12 U.S.C. § 3414(a)(5)(A) (2006); Rosen, *supra* note 23 (“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.”).

²⁴⁴ 18 U.S.C. § 3511 (2006).

²⁴⁵ 15 U.S.C. § 6802(e)(8).

²⁴⁶ *E.g.*, *United States v. Gross*, 416 F.2d 1205, 1212-1213 (8th Cir. 1969); *Harris v. United States*, 413 F.2d 316, 317-318 (9th Cir. 1969); *Galbraith v. United States*, 387 F.2d 617, 618 (10th Cir. 1968); *Interstate Commerce*

comparable force of law – a judicially decreed order – unless they are challenged and subsequently upheld in court.²⁴⁷ Hence, permissive compliance to NSLs does not fall within the strict confines of the “as compelled by law” language adopted by many banks in their privacy agreements.²⁴⁸ Furthermore, blind acquiescence to the whims of law enforcement does not meld with the case law in most states, which has limited the disclosure of customer records to authorities to subpoenas, summons, and other formal processes.²⁴⁹ In addition, releasing records without a hard look at the nature of the request and the requesting authority conflicts with banks’ promises to respect customer privacy and their self-assigned duty of confidentiality.²⁵⁰ This is particularly true when banks take on heightened obligations to their customers by serving in more intimate roles.²⁵¹

Courts should approach bank compliance with non-compulsory 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. In finding that banks could not grant the Internal Revenue Service informal access to bank records, the court determined that voluntary cooperation is not exempt from the requirements of the RFPA:

Comm’n v. Brinson, 154 U.S. 447, 485 (1894). *But see* Vera Bergelson, *It’s Personal But Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379 (2003).

²⁴⁷ 18 U.S.C. § 3511(c) (2006).

²⁴⁸ Winer, *supra* note 40.

²⁴⁹ *See infra* Subsec. III.C.2.b.

²⁵⁰ 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 Kansas state court accorded considerable weight to the fact that the law enforcement request was a subpoena. In that case, the Commissioner of the Securities and Exchange Commission had 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.” *Brant v. Bank of America*, 31 P.3d 952, 959 (Kan. 2001).

²⁵¹ *Pigg v. Robertson*, 549 S.W.2d 597 (Mo. App. 1977) (implying a confidential relation where bank employees were called upon to give advice to customers); 12 U.S.C. § 1813(f) (“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.”).

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.²⁵²

Similarly, the California courts rejected voluntariness 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."²⁵³

Before the Intelligence Authorization Act of 1987, the FBI could only issue such non-mandatory letters. A substantial number of financial institutions complied voluntarily. 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 or State banking privacy laws."²⁵⁴ Financial institutions which did not comply with the letters claimed that "State law prohibit[ed] them from granting access and the RFPA, since it permits but does not mandate such access, does not override State law" and feared that "cooperation might expose them to liability to the customer to whose records the FBI sought access."²⁵⁵ 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

²⁵² *Neece v. IRS*, 922 F.2d 573, 576 (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.").

²⁵³ *Burrows* at 590.

²⁵⁴ The House committee did not speak directly to the potential for liability under the original § 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 records for counterintelligence purposes in certain circumstances, [§ 404] preempts State law to the contrary which otherwise would not permit such access." H.R. Rep. 99-690(I), *supra* note 80, at 14-15.

²⁵⁵ *Id.* 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." H.R. Rep. 99-690(I), *supra* note 80, at 17.

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 precedent 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 regimes²⁵⁶ or self-generated promises of privacy. Hence, banks should be required to institute a policy of challenging non-mandatory national security letters or at least engaging in critical review to determine the whether NSLs should be challenged on a case by case basis.

B. When do depositors have a right against banks that banks 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.²⁵⁷ Although courts have almost unanimously held that subpoenas are

²⁵⁶ See *infra* Sec. III.B.

²⁵⁷ Testimony of former Attorney General John Ashcroft, *supra* note 226.

considered compulsion by law²⁵⁸ and bank-customer privacy agreements typically allow for disclosure under such circumstances,²⁵⁹ the 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 by their construction as contracts of adhesion.²⁶⁰ Since 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.²⁶¹ These contracts merit greater deference when they conform to publicly determined standards.²⁶² In this case, the Reauthorized Patriot Act evinces that Congress is espousing a policy permitting banks to challenge FISA requests.²⁶³ Given this development, courts should not be strong-armed by banks unilaterally limiting their obligations to customers through adhesive contracts. 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 like *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 truer in the case of an NSL, which is not subjected to pre-enforcement judicial review and hence should not be considered compulsion by law.²⁶⁴ Finally, non-mandatory NSLs are by

²⁵⁸ See *infra* Subsec. III.C.2.b.

²⁵⁹ See *infra* note 242 and accompanying text.

²⁶⁰ Rakoff, *supra* note 170, at 1176-80; see generally *infra* Subsec. III.C.3.

²⁶¹ Korobkin, *supra* note 177, at 1233.

²⁶² Slawson, *supra* note 179, at 536.

²⁶³ 50 U.S.C. § 1861(f); 18 U.S.C. § 5311.

²⁶⁴ See *infra* Sec. II.B.

definition not compulsory in nature.²⁶⁵ When the issuing agency requests records on an admittedly optional basis, courts should be reluctant to hold that banks may comply pro forma despite the promises their relationships with their customers.²⁶⁶

V. Contracting to require challenges

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 has only created uncertainty for customers, who have no way to predict whether a bank would challenge requests for their records and under what circumstances.²⁶⁷ 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 considering personal valuations of financial privacy, the "golden mean" is "a solution tailored to individual preferences and values."²⁶⁸

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

²⁶⁵ See *infra* Sec. II.C.

²⁶⁶ E.g., *Neece v. IRS*, 922 F.2d 573, 576 (10th Cir. 1990).

²⁶⁷ Steven A. Bibas, *A Contractual Approach to Data Privacy*, 17 HARV. J. L. & PUBLIC 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 efficiently and tailor the law to meet their needs.").

²⁶⁸ *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 (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.").

cannot be “compelled” to disclose information by an unlawful request.²⁶⁹ 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.²⁷⁰

A. Terms?

As discussed in the preceding section, privacy agreements as currently drafted may obligate banks to challenge some law enforcement inquiries in light of duties accrued from statutory protections and or the banking tradition of confidentiality. However, the tenuous nature of these financial privacy protections provides questionable assurance of privacy for customers at best.²⁷¹ In light of the recent procedural nod to 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. 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

²⁶⁹ *E.g., State v. Thompson*, 810 P.2d 415, 419 (Ut. 1991).

²⁷⁰ 50 U.S.C. § 1861(e) (2006) (“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.”).

²⁷¹ Edgar & Walczak, *supra* note 262, at 22 (providing statistics which imply that ex ante judicial review is merely a rubber stamp).

served, whether it describes the solicited documents with enough particularity, and whether the requested production would be unduly burdensome.²⁷² Since Congress has already proclaimed that these challenges are not incompatible with law enforcement investigations,²⁷³ financial institutions and their customers should be able to build this procedural hook into their contracts explicitly.

Since 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.²⁷⁴ 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.”²⁷⁵ 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 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.” The court found the doctor’s “cho[ice] to limit his ability to share information” dispositive in overriding the norms of disclosure.²⁷⁶ In holding the doctor liable for breach of confidentiality, the court noted the public policy favoring “the free-flow of

²⁷² 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).

²⁷³ 50 U.S.C. § 1861(f) (explicitly authorizing banks to bring these challenges).

²⁷⁴ *Teeling v. Ind. Nat’l Bank*, 436 N.E.2d 855 (Ind. 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.”)

²⁷⁵ *Sindlinger v. Dep’t Fin. Inst.*, 199 N.E. 715 (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.”).

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

information in a truth-finding process” but that an adhered party cannot voluntarily testify to protected information.²⁷⁷

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.²⁷⁸ 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 FRPA 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. 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.”²⁷⁹ This principle of self-determination – allowing customers to take charge of the flow of their person and to play a role in the decisions governing the dissemination of their records among an array of presented options – would translate well into context of contracting for pre-enforcement challenges.

²⁷⁷ *Id.* at 497. However, in other contexts such as employee trade secret agreements, “courts 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 involved.” *McGrane v. Reader’s Digest Assoc.*, 822 F. Supp. 1044, 1052 (S.D.N.Y. 1993).

²⁷⁸ 15 U.S.C. § 6803(a).

²⁷⁹ Division of Financial Practices, “Gramm-Leach-Bliley Act: Privacy of Consumer Financial Information,” Federal Trade Commission (June 18, 2001), <http://www.ftc.gov/privacy/glbact/glboutline.htm>; *see also* Swire, *supra* note 48, at 1263.

B. 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.²⁸⁰ These exceptions are written narrowly and interpreted as such by the courts.²⁸¹ 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 process.²⁸² These cases typically get litigated because bank customers have standing under the Financial Right to Privacy Act when banks divulge information despite the failure of the requesting authority to comply with the Act's procedural requirements.²⁸³ 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.²⁸⁴ In investigations concerning national security, however, customers cannot be notified that their records have been subpoenaed. Hence, they must rely on banks to vindicate their rights.

²⁸⁰ *E.g.*, 15 U.S.C. § 6802(e)(8).

²⁸¹ *See infra* Sec. III.B; 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 (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.”).

²⁸² *E.g.*, *Neece v. IRS*, 922 F.2d 573, 576 (10th Cir. 1990).

²⁸³ Customer Challenge Provisions, 12 U.S.C. 3410 (2000) (“Within ten days of service or within fourteen days of mailing of a subpoena, summons, or formal written request, a customer may file a motion to quash an administrative summons or judicial subpoena, 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.”).

²⁸⁴ *Anderson v. La Junta State Bank*, 115 F.3d 756 (10th Cir. 1997) (citing the narrow exceptions to 12 U.S.C. § 3402); *see also Neece*, 922 F.2d at 574 (“12 USC § 3402 of the RFPA specifies the only means by which federal agencies can obtain an individual's records in the possession of third party recordkeepers such as financial institutions.”).

Customers have standing to object when banks disclose records of their own volition, without formal process by the requesting authority.²⁸⁵ 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 which were produced in a different time and place than specified in the subpoena: “The 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.”²⁸⁶ Banks also have standing to bring a motion to quash a subpoena directing them to release customer records.²⁸⁷

While customers do not have standing under the RFPA or other federal statutes to move to suppress evidence obtained from unauthorized or unlawful disclosures,²⁸⁸ 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.²⁸⁹ 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

²⁸⁵ *Id.* 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.” The 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. *California Bankers Association v. Schultz*, 416 US 21, 51 (1974).

²⁸⁶ *Bond v. Slavin*, 851 A.2d 598, 608 (Md. 2003) (holding that subpoenaed records should not have been delivered to P’s wife instead of the court without a hearing) (citing *Banks v. Conn. R. & Lighting Co.*, 79 Conn. 116, 118-19 (1906)). 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.

²⁸⁷ *Lincoln Bank v. Okla. Tax Comm’n*, 827 P.2d 1314 (Okla. 1992),

²⁸⁸ *E.g., In re Special Investigation No. 242*, 452 A.2d 1319 (Md. 1982) (holding that customer does not have standing to challenge a subpoena that was not directed at him, but rather to the bank to which he had voluntarily disclosed info).

²⁸⁹ *Charnes v. DiGiacomo*, 612 P.2d 1117, 1120 (Colo. 1980) (citing COLO. CONST. Art. II, Sec. 7).

violation of a state financial privacy statute.²⁹⁰ State courts in Utah and Arizona have heard customer challenges and similarly granted motions to suppress financial records obtained through unlawful subpoenas on state constitutional grounds.²⁹¹ 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.²⁹² The Illinois court found that the most appropriate means of balancing the personal interest in privacy against the public interest in effective investigations was using the validity of the subpoena as the test.²⁹³

The newly created ability of banks to raise objections to FISA requests is drafted in the Reauthorized Patriot Act as a privilege. However, there is precedent for the argument that this privilege may become a duty under certain circumstances. For example, in the case of a subpoena seeking “confidential supervisory information” from the Federal Reserve Bank, persons seeking to compel inspection or production of records “must file a written request with the Board’s general counsel showing that the need for confidential information outweighs the

²⁹⁰ *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.”); *State v. Flynn*, 464 A.2d 268, 274 (N.H. 1983) (“Therefore, we hold that the defendant has standing to challenge any evidence obtained directly or indirectly from a violation of his privacy rights . . . [I]nformation wrongly obtained from the defendant’s accounts . . . may be suppressed.”).

²⁹¹ *State v. Thompson*, 810 P.2d 415, 419 (Ut. 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 (Ut. 1990); see also *State v. Bolt*, 689 P.2d 519, 524 (Ariz. 1984) (same holding based on parallel provision in Arizona state constitution).

²⁹² ILL. CONST. 1970, 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. 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 Section 141.1(d)(1) of the Illinois Banking Act. (Ill. Rev. Stat.1979. ch. 16 1/2, par. 148.1(d)(1)) (providing state statutory right to privacy and notice).

²⁹³ *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 (S.C. 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).

need to maintain confidentiality.”²⁹⁴ More generally, courts in many jurisdictions have agreed that banks have standing to challenge subpoenas on behalf of their customers.²⁹⁵ These challenges to law enforcement inquiries in other contexts have set the stage for banks using 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. 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.”²⁹⁶ Bank of America then received a subpoena requesting the production of customer records and prohibiting disclosure of the request to any third party. The bank challenged the subpoena on the grounds that compliance would violate customers’ Fourth Amendment right to privacy. However, the Kansas state court held that “the right to privacy statement . . . does not create a privacy expectation in situation such as this where the agency is empowered to conduct an investigation in private.”²⁹⁷ 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

²⁹⁴ *FDIC v. Flagship Auto Cntr.*, 2005 U.S. Dist LEXIS 9468 (N.D. Oh. May 13, 2005) (citing 12 CFR § 261.22(a), (b) (2005)).

²⁹⁵ *Lincoln Bank & Trust Co. v. Okla. Tax Comm’n*, 827 P.2d 1314 (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).

²⁹⁶ *Brant v. Bank of America*, 31 P.3d 952, 954 (Kan. 2001).

²⁹⁷ *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.”).

of the subpoena.”²⁹⁸ Hence, the court was not promulgating a blanket rule that privacy agreements could not be used to expand privacy protections, but rather saying that the privacy agreement in question as written did not determinatively expand confidentiality into the circumstances of the case.²⁹⁹ 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. 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.³⁰⁰

Generally, the subject of a subpoena directly receives the subpoena and has an opportunity to challenge it by filing a motion to quash.³⁰¹ 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.”³⁰² Under these circumstances, banks should rise to the occasion and defend their customers’ privacy as Congress has newly 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.

C. Public policy

²⁹⁸ *Id.*

²⁹⁹ However, the court does generally come out in favor of allowing private investigations. *Brant*, 31 P.3d at 955 (“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).

³⁰⁰ *Rush v. Maine*, 387 A.2d 1127 (Me. 1978).

³⁰¹ FED. R. CIV. P. 45(c)(3)(A).

³⁰² Schulhofer, *supra* note 59, at 545.

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.”³⁰³ 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. The only requirements which cannot be circumvented by contract are “good faith, diligence, reasonableness, and care.”³⁰⁴ These unalterable principles may serve as guideposts in determining whether bank-customer agreements obligating the bank to 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] promise or other term of an agreement is unenforceable on grounds of public policy if legislation provides that it is unenforceable or the interest in its enforcement is clearly outweighed in the circumstances by a public policy against the enforcement of such terms.”³⁰⁵ 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.”³⁰⁶

³⁰³ *Teeling v. Indiana Nat’l Bank*, 436 N.E.2d 855, 858 (Ind. Ct. App. 1982) (customer alleging that bank failed to provide sound investment advice).

³⁰⁴ U.C.C. § 1-102(3) (2005).

³⁰⁵ RESTATEMENT (SECOND) OF CONTRACTS § 178(1); *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.”).

³⁰⁶ *Id.* § 178(3); Richard A. Lord, *The Various Foundations of Public Policy*, 5 WILLISTON ON CONTRACTS § 12:2.

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.³⁰⁷ Courts also hesitate to punish someone for exposing the wrongdoing of another. As a result, contracts preventing the disclosure of information pointing to the perpetrator of a crime are seldom enforced. Courts have formalized this public policy exception by carving out from enforceability contracts which intend to defraud or deceive third parties.³⁰⁸ 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 element of intent or knowledge.³⁰⁹ These carve-outs “indicate the law’s reluctance to enforce contracts which have the effect of injuring third persons, whether such possibility is anticipated or not.”³¹⁰ 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.”³¹¹

³⁰⁷ 17A AM.JUR.2D CONTRACTS § 273, at 276-77 (1991) (“All agreements tending to suppress legal investigations concerning offenses, or agreements stifling criminal prosecutions, are illegal.”); 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”).

³⁰⁸ 6A CORBIN ON CONTRACTS § 1455; RESTATEMENT OF CONTRACTS § 577; *e.g.* *Lachman* (“An agreement, the purpose of which is the commission of a civil wrong against a third party, is also illegal.”) (citing *Singer Sewing Mach. Co. v. Escoe*, 64 P.2d 855 (Okl. 1937), which typifies the type of contract entered into for the purpose of concealing a crime); *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.”).

³⁰⁹ 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 v. Sperry-Sun Surveying Co.*, 457 F.2d at 853 (10th Cir. 1972).

³¹⁰ *Id.*; *see also Singer Sewing Machine Co. v. Escoe*, 64 P.2d 855 (Okl. 1937); *Wilshire Oil Co. v. Riffe*, 409 F.2d 1277 (10th Cir. 1969).

³¹¹ *Lachman*, 457 F.2d at 854.

In an analogous context, courts have also voided on public policy grounds settlement agreements that barred the reporting of crimes to the relevant law enforcement agencies. Courts have even resisted enforcing settlement agreements which not explicitly conflict with the letter of the law if they generally prevent the revelation of suspicious activity to authorities. In refusing to uphold a settlement agreement that purportedly barred reporting crimes to German authorities, the Federal Circuit acknowledged that “there is no federal statute, treaty, or constitutional requirement mandating the referrals to the German law enforcement authorities.” 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.”³¹²

However, in considering whether a contract is void as against public policy, it is important to remember that there are competing policies at stake.³¹³ 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.”³¹⁴ In the case of bank customers, the first two factors are weighted toward enforcing privacy agreements. As Congress indicated in passing the Right to Financial Privacy Act, customers reasonably expect that the information they are required to convey to banks to participate in financial transactions will be

³¹² *Fomby-Denson v. Dep't of Army*, 247 F.3d 1366, 1375 (Fed. Cir. 2001) (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) (historic duty of citizens to report crimes).

³¹³ *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).

³¹⁴ RESTATEMENT (SECOND) OF CONTRACTS § 178 comment b (1979).

kept as confidential as is legally permissible.³¹⁵ Furthermore, the forfeiture of financial privacy is an irreparable harm that would foreseeably result 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.”³¹⁶ Public policy and unconscionability are an 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.³¹⁷

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 cabined 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, the 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.³¹⁸ 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.”³¹⁹ In deciding

³¹⁵ H.R. Rep. No. 95-1383, *supra* note 68, at 28.

³¹⁶ Symons, *supra* note 70, at 240.

³¹⁷ U.C.C. § 1-304 (see text accompanying note 203); § 1-210(b)(20) (defining good faith as “honesty in fact and the observance of reasonable commercial standards of fair dealing”); Comment 4 to § 3-103 (explaining that the good faith standard requires “fairness of conduct,” not merely the exercise of due care).

³¹⁸ *Banaitis v. Mitsubishi Bank*, 879 P.2d 1288, 1294 (Ore. 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 relevant ‘evidence’ of a particular public policy, whether that be expressed in constitutional and statutory provisions or in the case law of this or other jurisdictions.”).

³¹⁹ Carol M. Bast, *At What Price Silence: Are Confidentiality Agreements Enforceable?*, 25 WM. MITCHELL L. REV. 627, 635 (1999); *id.* at 649 (“[D]isclosures to law enforcement agents were privileged because they were in the public interest.”); *see also Re v. Horstmann*, 1987 WL 16710, at *2 (Del. Super. Aug. 11, 1987) (finding no damages for breach of non-disclosure agreement for employee to breach confidentiality agreement to report

whether to enforce these agreements, states consider factors such as whether the restrictions are “no broader than is necessary,” “reasonably related to the protection of the information,” “reasonable from the standpoint of public policy,” and “factors of time and the nature of the business interest sought to be protected.”³²⁰ 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 require banks to challenge law enforcement inquiries on behalf of their customers are enforceable and under what circumstances.

Furthermore, unlike the contracts which 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.³²¹ 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 cooperating with the Equal Employment Opportunity Commission. In finding that the agreement was not void as against public policy, the court found persuasive that the provision did not prevent the plaintiff from testifying in response to a subpoena.³²² Similarly, in this case, the proposed bank agreements would not bar disclosure altogether, but would only apply congressionally-sanctioned safeguards to individual cases.

securities violation); *Baker*, 117 S. Ct 1310 (1997) (providing a similar holding in the products liability context because state public policy favored disclosure of nonprivileged and relevant information.).

³²⁰ *Id.* at 640-42.

³²¹ *Compare Equal Employment Opportunity Comm’n v. Astra*, 94 F.3d 738, 744 (1st Cir. 1996) (“In performing the balancing here, we must weigh the impact of settlement provisions that effectively bar cooperation with the EEOC on the enforcement of Title VII.”).

³²² *Hoffman v. United Telecomm.*, 687 F. Supp. 1512 (D. Kan. 1988) (“[T]he settlement provision was not contrary to public policy, especially because the provision allowed Hoffman to testify under subpoena.”).

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 of bank challenges 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.

Appendix I: Market?

In Section V, this Paper addressed the enforceability of contracts wherein banks would promise to challenge subpoenas on behalf of their customers. In this Appendix, 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. 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.³²³

When courts have awarded attorney's fees for time spent preparing a motion to quash a subpoena, they have usually found awards around \$5,000 to be reasonable.³²⁴ To be generous, let us estimate that it would cost a bank \$10,000 in attorney hours to challenge any given request for customer records. In 2005, there were approximately 2,000 FISA requests. Only a fraction of

³²³ 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 communication service providers unless they provide specific services, and for other purposes, *The Week in Congress* (Mar. 10, 2006),

http://www.theweekincongress.com/Member/MAR06_FULL/S2271PATRIOTshMAR10.htm.

³²⁴ *E.g.*, *In re Mullins*, 87 F.3d 1372 (D.C. Cir. 1996); *Panico v. Panico*, 2006 WL 3703399, at *3 (Ohio App. Dec. 14, 2006); Motion to Quash and/or Limit Subpoena Duces Tecum, *In the Matter of N. Tex. Specialty Physicians*, <http://www.ftc.gov/os/adjpro/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.").

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.³²⁵ At least seventy-five percent of these individuals are estimated to have some form of bank account.³²⁶ Accordingly, there are at 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 only 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.³²⁷ 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 only average out to be \$6.67 per customer. Given the gravity of concern for financial privacy evinced in surveys of the American public,³²⁸ it seems almost certain that many customers would value this additional safeguard on their privacy enough to pay at least this much for it.³²⁹ Furthermore, the widespread concern for financial privacy suggests that these

³²⁵ Julie Meyer, Age: 2000, Census 2000 Brief (October 2001), <http://www.census.gov/prod/2001pubs/c2kbr01-12.pdf>.

³²⁶ Lawrence H. Summers, Secretary of the Treasury, Remarks to the Enterprise Foundation's Annual Enterprise Network Conference (Oct. 13, 1999), <http://www.ustreas.gov/press/releases/ls153.htm> (estimating that "between 10 and 20 percent of American households still do not have any type of transaction account").

³²⁷ For a general discussion of adverse selection, see KENNETH S. ABRAHAM, INSURANCE LAW & REGULATION 6-7 (4th ed. 2005).

³²⁸ *E.g.*, Thorsberg, *supra* note 150 (discussing PC World survey).

³²⁹ *See generally* Bibas, *supra* note 267 (discussing how prices take into account individual subjective valuations and reflect consumer preferences).

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 government inquiries on their behalf, the price per customer will be only 26 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.