5 Privacy and Confidentiality[1]

The wire transfer monitoring systems proposed in chapter 7 share the feature of increasing government access to wire transfer records. Wire transfers are the medium of choice for large corporate payments requiring immediacy, security and certainty, and wire transfers are a vital part of the operation of the modern industrial and service economies of the United States and the world. Corporations use wire transfer systems to move capital, buy stocks and pay for international and domestic trade. Private parties also use the wire transfer medium to move money expeditiously, and some experts forecast that individuals will increasingly come to utilize wire transfers as an integral part of home banking, although the advent of digital money may prove a more facile means of moving money in the future (see box 7-4 in chapter 7).

[1] This chapter and the next will use the term "confidentiality" to refer to relationships wherein parties, contractually or otherwise, keep information secret. "Security" refers to safeguards undertaken to prevent unauthorized access to information. "Privacy" refers to policy debates regarding the balance struck between the interests of individuals in liberty and the interests of society in a stable social order. This balance is struck in court cases and legislation and is always subject to modification. Consider the recent bombing in Oklahoma City. According to the *Washington Post*, the government wishes to create a counterterrorism center, with a new mission of "intercepting digital communications." *Washington Post*, June 11, 1995, p. F7. This, and the antiterrorism bill nearing enactment, will likely reduce individuals' privacy in electronic communications.

One significant difference between enhanced counterterrorism measures and the monitoring of wire transfer systems would be that in the former case, arguably all citizens will have a reduced expectation of privacy and all citizens will benefit (i.e., from a reduced threat of terrorism). In the case of wire transfers, however, a small set of parties will have their confidentiality compromised and receive little, if any, direct benefit in return. Society as a whole benefits from reduction in the amount of money laundering, while the costs of that reduction are borne by a limited set of actors.

Each of the configurations discussed in chapter 7 would increase the government's access to domestic wire transfer records, with little or no requirement of individualized suspicion. Some configurations would require government collection and retention of an unprecedented volume of data; the government would come to possess a great chunk of the financial aspect of the stream of commerce. This access first represents an archetypal communications privacy issue, harking back to court cases such as *Berger* v. *New York* and *Katz* v. *United States* and the legislative debates surrounding wiretapping, from Title III of the Omnibus Crime Control and Safe Streets Act of 1968 to the recent Communications Assistance for Law Enforcement Act of 1994.[2] Second, government access to wire transfer records would represent a substantial diminution in financial privacy. Third, the subsequent manipulation of the wire transfer data, relating them to other financial or personal data, is computer matching—a practice termed by one noted commentator as "one of the most vexing privacy issues of the 1980s" and "one of the most virulent forms of surveillance practiced by any government."[3] In either case, some of the proposed technological configurations conjure up the image of the computer state, where all data, no matter how innocuous or elliptical in itself, may be collected, aggregated, manipulated, and cross-correlated with other databases to the point where it becomes information with a context and no longer innocuous.[4]

Privacy commentators bring different viewpoints to the privacy and confidentiality issues raised by the wire transfer monitoring proposals. Some privacy advocates view this question primarily as governed by Constitutional standards and policy, articulated by the Fourth Amendment and 200 years of jurisprudence and legislative enactments, finetuning the balance between the interests of law enforcement and the individual. Other commentators, influenced by "fair information practices," view this problem as primarily one of impermissible "secondary use," or the injunction against the use of information beyond the purpose for which it was collected (see box 5-1).[5] Both groups of privacy advocates would be

---

[2] *Berger,* 389 U.S. 41 (1967), *Katz,* 389 U.S. 347 (1967)(*Berger* and *Katz* were the Supreme Court's watershed decisions to extend Fourth Amendment protections to telephonic communications); Title III, Pub. L. 90-351 (June 19, 1968)(the legislative response to *Katz* and *Berger*); the Communications Assistance for Law Enforcement Act of 1994, Pub. L. 103-414 (Oct. 25, 1994), requiring the telecommunications industry to assist law enforcement agencies in matching intercept needs with modern communication technology. See the OTA report *Electronic Surveillance in a Digital Age*, analyzing the costs associated with facilitating law enforcement wiretapping of digital switches. U.S. Congress, Office of Technology Assessment, OTA-BP-ITC-149 (Washington, DC: U.S. Government Printing Office, July 1995).

[3] David H. Flaherty, *Protecting Privacy in Surveillance Societies: the Federal Republic of Germany, Sweden, France, Canada, and the United States* (Chapel Hill: The University of North Carolina Press, 1989), p. 344. "The current enthusiasm for matching programs is a typical search for a simple panacea for large problem that in some ways are almost hopeless; the enthusiasm is even greater, at least for a time, because the 'fix' is technological." *Ibid.* at 345. Flaherty focuses on the loss of individual liberty through governmental computer matching/data linkages intended to root out fraud and abuse of government benefits programs. Another author underscores the threat to privacy posed by computer matching. John Shattuck, "In the Shadow of *1984*: National Identification Systems, Computer-Matching, and Privacy in the United States," 35 *Hastings Law J.* 991-1005, pp. 991-2 (July 1984)(noting also the Internal Revenue Services's (IRS) planned use of commercial data bases to generate lifestyle profiles to catch tax cheats). It should be noted that the Computer Matching Act and Privacy Protection Act of 1988 does not apply to law enforcement/national security matching of records.

[4] One noted information privacy expert, Professor Joel Reidenberg of Fordham Law School, goes further and terms any wire transfer monitoring proposal a "quantum leap towards the surveillance state."

[5] In 1973, the former Department of Health, Education, and Welfare articulated one of the earliest versions of the principles underlying fair information practices. The third principle stated that "there must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent," a classic formulation of the injunction against secondary use. U.S. Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* (Washington, DC: 1973), p. 41, *cited in* The Privacy Protection Study Commission, *Personal Privacy in an Information Society* (Washington, DC: 1977), p. 15, fn. 7.

BOX 5-1: Fair Information Practices and the Fourth Amendment

Fair information practices limit the secondary use of data, independent of the nature of the data subject and independent of the party conducting the secondary use. The Europeans have taken the lead in the application of fair information practices, although in the early 1970s, the United States promulgated the former Department of Health, Education and Welfare and Office of Management and Budget fair information practices guidelines governing information practices in the federal government. Reidenberg and Gamet-Pol applaud European data protection laws for their comprehensive treatment of the balance between information privacy and the freedom of information.[1] These authors suggest that the United States' piecemeal and sometimes inadequate guarantee of information privacy is coming under the active interest of the Europeans, and that the U.S. will have to start responding to this foreign trend in order to avoid lost business opportunities by the U.S. information industry.[2]

Corporations in the United States have incorporated fair information practices into their charters and bylaws to regulate their treatment of information. Questions remain whether fair information standards should extend to cover individuals *and* corporations, or even whether corporations themselves desire the protections. While individuals may share with corporations the fear that information about them may be manipulated to their economic detriment, individuals and corporations share few other concerns, such as the individual's desire for physical safety, avoidance of embarrassment or hurt feelings (protected by the tort of public disclosure) and for freedom to communicate political thinking without fear.

The further question arises whether the prohibition against secondary use should govern law enforcement conduct. Advocates in favor of extending the scope of fair information practices to criminal matters have the burden of squaring fair information practices with this country's long tradition of applying the Fourth Amendment to decide the question of what information may be properly gathered and used against criminal defendants. Thus far, this case has not been made, apart from the argument that European data protection standards may prove an impediment to U.S. corporations seeking to transfer and process data across international borders. While the European Union (EU) has made a point of treating public and private data protection equivalently, the pending EU Data Protection Directive contains two provisions contemplating special treatment of law enforcement and its need to process data to conduct its mission. (See chapter 6 for more detail on the international aspects of data protection.)

[1] Joel Reidenberg and Françoise Gamet-Pol, "The Fundamental Role of Privacy and Confidence in the Network," 30 *Wake Forest L. Rev.* 105-125 (Spring 1995), p. 117.

[2] *Ibid.*, p. 119.

SOURCE: Office of Technology Assessment, 1995.

alarmed by the loss of control over personal information and fears of inaccuracy and obsolescence in collected data.[6]

Ordinarily, recourse to analogy helps guide analysis of new problems in policy and law. But in this case, while many analogies may be suggested,

[6] It should be noted at the outset that individuals no longer own, possess or even enjoy dominion over their personal data. See, e.g., Shattuck, "Computer-Matching," *op. cit.*, footnote 3, p. 995. Doctrines of "information privacy" and "data protection" are an attempt to restore some control to the individual over data identifying the individual. See, Office of Management and Budget, National Information Infrastructure *Draft Principles for Providing and Using Personal Information*, 60 *Fed.Reg*. 4362, 4363 (January 20, 1995)("information privacy" defined as "an individual's claim to control the terms under which personal information—information identifiable to an individual—is obtained, disclosed and used").

none are completely apposite. Already, two analogies have been suggested—wiretapping and computer matching. Neither fully captures the nature of wholesale wire transfers and all the issues inherent in some of the technological configurations. Other possible analogies for a "screening" system include: a) sobriety checkpoint roadblocks, as litigated in *Sitz* v. *Michigan State Department of Police*;[7] b) the airport courier drug profile;[8] and c) the questioning of passengers on a stopped long-haul bus, *Florida* v. *Bostick*.[9] While these analogies raise the idea of the "profile," a set of characteristics putatively separating the innocent from the suspicious, they all fail in one respect. They do not capture the fact that most of the technology configurations would retain funds transfer data, perhaps even wire transfers not immediately associated with some profile as "suspicious."

That the dominant users of the various wire transfer systems are currently corporate further complicates the analysis. Compared to the individual right of privacy, the corporation enjoys only a reduced right of confidentiality—a right premised on a concern for economic detriment through the loss of confidential business information. Recent court cases and legislation have confirmed the merits of conferring on corporations some measure of protection, however.[10] For many commentators, particularly those who anchor the right to privacy on its role in preserving the free exchange of political ideas, the corporation's privacy interests in this matter may amount only to a feather's weight, as set against "the stone" of the law enforcement interest in stemming the flow of illicit money.[11] There are others, however, who fashion a principled basis for finding a corporate interest in confidentiality, particularly Judge Richard Posner, who places a higher premium on corporate privacy than individual privacy.[12]

---

[7] 496 U.S. 444 (1990)(holding constitutional a police roadside blockade where all motorists along a highway were briefly detained and screened for signs of intoxication; some 1.5 percent were arrested out of those detained). *Sitz* is partially distinguished by the public nature of traveling on a highway; by contrast, current law provides a measure of confidentiality to domestic wire transfers in electronic transit and storage.

[8] Federal and local law enforcement agents have developed crude profiles setting forth characteristics of drug couriers traveling via airplanes, buses and trains. Agents scrutinize disembarking passengers against the backdrop of the profile, approaching those suspected of carrying narcotics and asking if they might search their baggage. See, e.g., *United States* v. *Sokolow*, 490 U.S. 1 (1989)(the agent's use of a "drug courier profile" to identify the defendant did not taint the detention and later arrest, even though the profile might be consistent with innocent behavior). A glaring dissimilarity here would be the agents' right to be in the public spaces of bus and train terminals and airports, in contrast to the currently confidential nature of wire transfer systems (consider that Fedwire requires subpoenas of even Federal Reserve employees before they may examine wire transfer records).

[9] 501 U.S. 429 (1991)(upholding the constitutionality of searches and seizures where agents boarded long-haul buses during scheduled stops and applied courier profiles to the passengers). Another analogy suggested is the Bank Security Act (BSA) data itself, e.g., the Ccurrency Transaction Report (CTR) and Currency or Monetary Instruments Report (CMIR), although these forms are distinguished by the fact that they are specifically created for the government, and not used outside of their intended purpose, namely the detection of money laundering and other forms of financial crime. Hence, they are not put to a troubling secondary use beyond their intended purpose.

[10] See *Tavoulareas* v. *The Washington Post Company*, 724 F.2d 1010, (D.C. Cir.); *vacated* and *remanded*, March 15, 1984; see also the Electronic Communications Privacy Act of 1986 (applying to individuals and corporations alike).

[11] Telephone interview with Professor Alan F. Westin, August 25, 1994. Westin recognizes the corporation's right to engage in the decision-making process in private, and, also, the right to associate with others privately.

[12] Richard Posner, *The Economic Analysis of the Law* (Cambridge, MA: Harvard University Press, 1981), p. 248. "Secrecy is an important method for the entrepreneur to appropriate the social benefits he creates, but in private life secrecy is more likely to operate simply to conceal discreditable facts." See also, George Trubow, "Whether and Whither Corporate Privacy," to be published in *DataLaw Report* and Anita L. Allen, "Rethinking the Rule Against Corporate Privacy Rights: Some Conceptual Quandaries for the Common Law," 20 *John Marshall L. Rev.* 607-639 (Summer 1987).

Some privacy advocates resist linking the terms "corporation" and "privacy,"[13] in part because the corporation lacks the psychological apparatus to take offense at intrusions into protected zones and perhaps, because historically privacy advocates have viewed direct marketing companies and other corporations as violating the privacy of individuals. Other privacy advocates influenced by fair information practices condemn all secondary uses of information, independent of whether the data is generated by a corporation or individual and regardless of whether government or corporations are scrutinizing data for the secondary purpose.[14] Some European nations, including Austria, Luxembourg and Norway, extend data protection principles to corporate entities. Yet fair information practices have not uniformly been adopted or practiced by U.S. corporations to protect consumers, so it would appear to be honoring the principle too much to extend their benefits to the corporation. Significantly, the Business Roundtable expressly demurred at protecting legal persons, or corporations, principally out of a fear that competitors could demand access to files held on them by other corporations, a central tenet of fair information practices.[15]

CONSTITUTIONAL AND LEGISLATIVE PERSPECTIVES ON FINANCIAL PRIVACY

Privacy Jurisprudence

United States v. *Miller*, 425 U.S. 435 (1976), remains the state of constitutional jurisprudence on the question whether individuals enjoy under the Fourth Amendment a "reasonable expectation of privacy" in financial records created or maintained by a bank in the course of ordinary business dealings.[16] In 1976, the Supreme Court answered the question in the negative. Some commentators have criticized the ruling as well as the incomplete attempt of Congress through the Right to Financial Privacy Act of 1978 (RFPA) to undo the effects of *Miller.* But the Supreme Court is unlikely to revisit the issue in the near future, because RFPA approximates the procedural protections of the Fourth Amendment for financial privacy and also because the *Miller* case rests on old and broad precedent undermining the ability of individuals to contest government access to records held by

[13] "Virtually everybody agrees that privacy, by definition, is uniquely a personal right. Artificial persons, as opposed to natural persons, do not enjoy a right to privacy." Robert Ellis Smith, *The Law of Privacy in a Nutshell* (Providence, RI: Privacy Journal, 1993), p. 48.

[14] The Code of Fair Information Practices, currently being updated by the Information Infrastructure Taskforce for the National Information Infrastructure under the aegis of the Office of Management and Budget (OMB), would also militate against secondary use of wire transfer data. *Draft Principles for Providing and Using Personal Information through the Office of Management and Budget*, 60 Fed. Reg. 4362 (Jan. 20, 1995).

[15] Business Roundtable Statement on Transborder Data Flow, *reprinted in* L. Richard Fischer, *The Law of Financial Privacy: A Compliance Guide* (2nd ed.)(Boston: Warren, Gorham & Lamont, 1991), 6-89, A6.3.

[16] The Fourth Amendment provides that the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

third parties, such as banks or accountants.[17] Some states have found state constitutional protection for financial records, however: in California, the state Supreme Court held that a customer "has a reasonable expectation that the bank would maintain the confidentiality of checks originated by the customer and of bank statements generated by the bank."[18] Today, the federal and California state protections for financial information are roughly equivalent, although they originated from opposing constitutional starting points.[19]

Nevertheless, it is useful to scrutinize the roots of the Fourth Amendment and its interpretations to weigh the intrusion of government access to payment systems information. Specifically, some argue that in the Fourth Amendment and the Bill of Rights generally the Founding Fathers sought to guard against the excesses of law enforcement tactics used by European nations, particularly the general warrant and writs of assistance: John Adams wrote that, when James Otis argued against general writs in 1761, "the child Independance [sic] was born."[20] (See box 6-1 in chapter 6 for discussion of a modern case with general subpoena implications.)

Alan Westin, in his seminal *Privacy and Freedom*, catalogs the values protected by the Bill of Rights, from the First Amendment and Justice Story's solicitude for "private judgment" and "private sentiment" to the concern for the home as a

---

[17] The *Miller* Court held that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by [the third party, or bank] to government authorities. . . ." 425 U.S. at 443. *Miller* follows *First National Bank* v. *United States*, 267 U.S. 576 (1925) and *Donaldson* v. *United States*, 400 U.S. at 522 (both cases holding that a summons served upon third parties violates the Fourth Amendment rights of neither the target nor the third party); see also *California Bankers Ass'n* v. *Shultz*, 416 U.S. 21 (1974), insofar as *Shultz* reaches the merits of privacy issues. In addition, the Supreme Court underscored the vitality of *Miller* in 1984, when it ruled that an individual had no reasonable expectation of privacy in confidential financial records given to and maintained by broker/dealer firms. *S.E.C.* v. *Jerry T. O'Brien, Inc*., 467 U.S. 735 (1984). At the core of these decisions lies the judicial finding that the individual does not own or possess the records that are held by a third party business. *Miller*, 425 U.S. at 440 (the customer "can assert neither ownership nor possession" of the records—in fact they are business records of the bank). Within two years, Congress responded to *Miller* with the RFPA. In contrast, when the Supreme Court found no constitutional right to be free from wiretapping in *Olmstead*, there was no express congressional response. Law enforcement wiretappings continued for forty years largely unfettered until the *Katz* decision and Title III circumscribed the practice of the telephonic wiretap, mandating a court order and special procedures to minimize the intrusion to legitimate telephonic conversations.

[18] *Burrows* v. *Superior Court*, 520 P. 2d 590 (Ca. Sup. Ct. 1974). *See also* Fischer, *The Law of Financial Privacy, op. cit.*, footnote 15, ¶5.04[4][a] (writing that Colorado, Florida, Illinois and Pennsylvania have followed the California rule, finding that state constitutions required legal process before access is permitted to bank-held financial information). Utah, California and Pennsylvania also confer some privacy rights to the corporation. It should be emphasized that although Congress may legislate based on the Commerce Clause and Supremacy Clause to pre-empt state constitutional protections, direct reversals by Congress of state constitutions are relatively rare. Article VI, clause 2 of the U.S. Constitution provides:

> This Constitution, and the laws of the United States which shall be made in pursuance thereof; and all treaties made, or which shall be made, under the authority of the United States shall be the supreme law of the land; and the judges in every state shall be bound thereby, any thing in the constitution or laws of any state to the contrary notwithstanding.

[19] Richard Fischer, OTA Workshop, Feb. 16, 1995. It should be noted at this juncture that the Fifth Amendment does not protect bank records either. The Fifth Amendment requires that documentary evidence be generated by the one claiming the Fifth Amendment right—not apposite in the financial records context. See, e.g., *Fisher* v. *United States*, 425 U.S. 391 (1976)(an individual cannot assert the Fifth Amendment to shield accountant-generated records from government subpoena).

[20] The Founding Fathers decried the general warrant and writ of assistance in the strongest of language, for "their indiscriminate quality, their license to search Everyman without particularized cause" (John Adams) and they were considered to be "the worst instrument of arbitrary power, the most destructive of English liberty, and the fundamental principles of law, that ever was found in an English law book," (John Otis), quoted by Nadine Strossen, "Individual Rights After *Sitz*," 42 *Hastings L.Rev.* 285, 353-54 (Jan. 1991). Strossen is particularly alarmed by this form of search, which is aimed not at gathering evidence on known wrongdoers, but rather at turning up previously unidentified and unsuspected offenders, *ibid.*, p. 355. The Founding Fathers were greatly concerned with the suspicionless entries into homes and businesses sanctioned by the general warrant and writs of assistance. In this view, the Framers intended that the Fourth Amendment prevent police from interfering with personal freedom unless the police had already formed particularized suspicion as to wrongdoing.

castle embodied in the antiquartering provision of the Third Amendment and the Fourth Amendment's express protection of papers and the home.[21] One may reasonably infer that the Bill of Rights places a premium on the sanctity of the mind and home, codifying a "rhetoric of domesticity" and the intellect, particularly political thoughts and speech.[22] Passages from Justice Brandeis's dissent in *Olmstead* v. *United States* confirm this view:

> The makers of our Constitution. . .recognized the significance of man's spiritual nature, of his feeling and of his intellect . . . . They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. 277 U.S. 438, 478 (1928).

And in a widely quoted prescient piece of his dissent, Brandeis notes:

> . . . the progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thought and emotions. *Ibid*., at 474.

More recently, in assessing the constitutionality of the Bank Secrecy Act (BSA) in the case of *California Bankers Ass'n* v. *Shultz,* the Court distinguished *Shultz* from *Stanford* v. *Texas*, where the Court had ruled that a warrant permitting the search and seizure of defendant's "books, records, pamphlets, cards, receipts, lists, memoranda, pictures, recordings and other written instruments concerning the Communist Party of Texas" was an unconstitutional general warrant.[23] Instrumental to the reasoning in *Shultz* was that the BSA data did not involve "rummaging around records of the plaintiffs, nor do the reports . . .deal with literary material as in *Stanford*; the information sought is about commerce, not literature."[24]

Thus, for nearly two centuries, the Supreme Court confined the scope of the Fourth Amendment to its plain text, to "persons, houses, papers, and effects." And in 1968, the Court extended the protections of the Fourth Amendment to "people not places," in protecting telephonic communication from a public phone booth.[25] But should the policies behind the Fourth Amendment further extend to and protect corporations and their financial communications in the stream of commerce?[26]

---

[21] Alan F. Westin, *Privacy and Freedom* (New York: Athenaeum, 1967), pp. 330-333. Westin's express linkage between privacy and freedom in the title intimates his emphasis upon the utility of privacy in maintaining a free and democratic society. This linkage is harder to perceive when the information is in the stream of commerce, of course.

[22] David J. Seipp, *The Right to Privacy in American History* (Cambridge, MA: Harvard University, 1978).

[23] 416 U.S. 21, 62 (1974).

[24] The specific Bank Secrecy Act (BSA) report discussed in *Shultz*, Foreign Bank Account Reports (FBARs), represent a mere fraction of the amount of international commerce that would be reported under any proposed monitoring system, weakening the precedential import of *Shultz*.

[25] This quoted phrase stems from *Katz* v. *United States*.

[26] Pre-electronic analogs for wire transfer payments would be checks, and for most of this nation's history, checks received no special protection from the scrutiny of law enforcement. At the same time, as is evident in the text, the telecommunications aspect of the wire transfer complicates the analysis, adding a concern for interception of electronic communications.

The Supreme Court's recent pronouncement on the Commerce Clause in *United States* v. *Lopez*, (No. 93-1260)(April 26, 1995) does not threaten Congressional power to regulate wire transfers. The *Lopez* Court held that the Gun-Free School Zones Act of 1990, which criminalized the possession of guns in a "school zone," exceeded Congressional authority to regulate commerce under the Commerce Clause of the federal Constitution and reaffirmed the federalism at the core of this Republic. Nevertheless, this ruling would not threaten the power of Congress to regulate wire transfers, which are close to the heart of interstate, and indeed, international commerce.

BOX 5-2: Major Supreme Court Cases on Privacy and Financial Privacy

- *Olmstead* v. *United States* (1928): The Supreme Court of the United States holds that the Fourth Amendment does not protect telephonic communications, even when the wiretap is achieved by physical trespass at the target's home.
- *Katz* v. *United States* (1967): Reversing *Olmstead*, the Supreme Court holds that the Fourth Amendment protects "people, not places," in finding that the bugging of a public telephone booth habitually used by the target of an investigation requires a warrant based on probable cause.
- *California Bankers Association* v. *Shultz* (1974): The Supreme Court upholds the constitutionality of the Bank Secrecy Act's reporting requirements, upholding the constitutionality of the Bank Secrecy Act against challenges based on the First Amendment right to privacy and anonymity in associations, the Fourth Amendment reasonable expectation of privacy and the deprivation of due process by imposition of unreasonable compliance costs on banks. It should be noted that the Court did not reach some of the most interesting arguments for purposes of wire transfer monitoring, to wit, whether depositors in excess of $10,000 had a Fourth Amendment violation to allege.
- *United States* v. *Miller* (1976): The leading case on financial privacy, in which the Supreme Court found no reasonable expectation of privacy and hence no Fourth Amendment protection for financial records held by third parties, such as financial institutions. This result is largely undone by the subsequent Congress, which enacted the Right to Financial Privacy Act, establishing a presumption of privacy in bank-held records.

SOURCE: Office of Technology Assessment, 1995.

In *Dow Chemical*, the Supreme Court obliquely suggested another constitutional issue.[27] The Supreme Court ruled that the government did not violate Dow Chemical Corporation's rights under the Fourth Amendment by flying over a manufacturing plant in a chartered plane and photographing the plant with commercial photographic equipment. The Court went on to suggest that if the government had not relied upon a commercial aviation photographer (by using alternatively a spy satellite, for example), perhaps the Court would have found that the corporation had a reasonable expectation of privacy. This suggests that the fact that the government observes a defendant from a legitimate vantage point (either from public airspace or from within the stream of commerce) does not insulate the government from charges of unconstitutional conduct: it is necessary to inquire as to the means of scrutiny. In the context of wire transfers and massive data matching by large computers, this line of analysis is partially undercut by the growing reliance of direct marketers on massively parallel computing for ever more sophisticated targeting of customers for their clientele. No longer is supercomputing the exclusive province of the federal government (see box 5-2).

The Statutory Picture

Any congressional decision on government access to wire transfer data will not be made *de novo*. Any of the technological configurations proposed in chapter 7 would represent a rollback of current privacy protections under law and would also represent a step back from the first recommendation of the U.S. Privacy Protection Study Commission, which recommended that Congress provide an expectation of confidentiality in records held by financial institutions, requiring that govern-

[27] *Dow Chemical Co*. v. *United States*, 476 U.S. 226, 238-239 (1986). The relevant language from *Dow Chemical* is what lawyers refer to as *dicta*. *Dicta* is speculative reasoning not logically essential to the ruling in a case, and hence not binding upon future cases.

ment show clear proof of the relationship of any record sought and a violation of law.[28]

Federal and state legislation and judicial pronouncements on privacy have made data protection a "patchwork quilt."[29] In addition, section 1515 of the Annunzio-Wylie Anti-Money Laundering Act of 1992 mandated that the Secretary of the Treasury promulgate international wire transfer recordkeeping provisions and authorized the Secretary to "request" copies of international wire transfer records from banks.[30] This provision has not been tested yet, as the recently issued wire transfer recordkeeping regulation does not take effect until January 1, 1996. In addition, the U.S. Treasury Department has interpreted its authority under the BSA, specifically 31 U.S.C. 5314, as authorizing Treasury to issue regulations requiring specified banks to disclose "wire fund transfers" with foreign financial agencies.[31]

Neither section 1515 of Annunzio-Wylie nor the "targeting" regulation addresses government access to domestic wire transfer records. Neither has the judiciary squarely addressed this issue. Some experts believe that the Electronic Communications Privacy Act (ECPA)[32] should control the analysis and prohibits access to the information,[33] while others maintain that ECPA does not cover wire transfers at some points in their life cycle through various banks.[34] The Federal Reserve Board's Office of General Counsel and others believe that RFPA should be viewed as the paramount statute, although some federal courts have held that the Act does not protect all wire transfer information. At least one court has so ruled because the wire travels through banks and wire transfer instrumentalities in which neither the originator nor the recipient holds an account.[35]

The protections afforded by RFPA and ECPA differ in material respects, a byproduct of the United States' piecemeal approach to privacy protection. While RFPA, by its letter and judicial interpretation, does not accord its limited protections to corporations and partnerships of greater than five partners,[36] ECPA applies to all "users" of an "electronic communications service." The statutes also differ in terms of the degree of protection afforded information, as well as the procedural requirements that must be adhered to before the release of information to law enforcement. For instance, under some circumstances RFPA requires that notice be provided to the bank custom-

---

[28] The Privacy Protection Study Commission, *Personal Privacy in an Information Society, op. cit.*, footnote 5, pp. 362-363.

[29] Wayne Madsen, *Handbook of Personal Data Protection* (New York: Macmillan Publishers Ltd, 1992), p. 108.

[30] The Annunzio-Wylie Anti-Money Laundering Act of 1992 (Pub.L No. 102-550, Title XV), with section 1515 codified at 12 U.S.C. 1829b(b)(3).

[31] 31 C.F.R. 103.25(a) and (b)(2).

[32] Pub. L. 99-508. In short, ECPA created a reduced right of privacy in electronic communications, supplementing Title III's more robust protection of telephonic communications.

[33] This group includes the OCC and the Office of Legal Counsel, Department of Justice, which opined that ECPA, not RFPA, controls electronic access to Fedwire data, relying in part upon lower courts' holdings that RFPA does not address intermediary banks' actions with respect to wire transfers for non-customers. OLC Opinion by Dellinger, September 13, 1993. The opinion rules that no judicial process is necessary to access records once they have been transferred to microfiche.

[34] Some support for this latter position may be found in the recent Fifth Circuit case, *Steve Jackson Games*, to the extent that the court's non-intercept analysis for e-mail may be extended to the transmission of wire transfers. *Steve Jackson Games v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994); *Steve Jackson Games* v. *United States Secret Service*, 816 F.Supp. 432 (W.D.Texas 1993) (finding no interception of unread e-mail stored on an electronic bulletin board since the acquisition of the e-mail was not contemporaneous with its transmission).

[35] *United States* v. *Daccarret*, 6 F.3d 37, 51-52 (2nd Cir. 1993)(holding RFPA as not protecting defendant Daccarret *et al.*, in part because they did not maintain an account in their names at the intermediary banks from which the wire transfers were seized).

[36] The Privacy Act also extends its limited protections solely to individuals.

er before the record is released, giving the customer an opportunity to invoke judicial process to quash the disclosure to law enforcement.[37]

While the first title of ECPA protects against the interception of electronic communications, the Stored Wire Act, Title II of ECPA, concerns itself with communications in "electronic storage" and sets out restrictions on the conduct of "electronic communications service providers:"[38]

> Any person or entity providing an electronic communications service to the public may not knowingly divulge to any person or entity the contents of an electronic communication while that communication is in electronic storage. 18 U.S.C. 2702(a)(1), see also S. Rep. No. 99-541, at 37.

"Electronic storage" is a term of art, signifying:

> A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
>
> B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication. 18 U.S.C. 2510(17).

Reporting of wire transfer information, either while in temporary storage while in transit or afterwards while stored for backup protection would thus violate ECPA.[39] Neither ECPA nor its legislative history give a sense to how long "backup protection" may go on, so it could be argued that long-term electronic storage of wire transfer messages would not merit protection. Nonetheless, ECPA specifically protects messages stored for more than 180 days and the wire transfers most interesting to law enforcement are apt to be relatively fresh, in any case.

The statute permits disclosure to law enforcement upon issuance of a court order, warrant or administrative subpoena, depending on the duration of the electronic storage.[40] (See box 5-3). If the electronic service provider, in this case a bank, inadvertently reads the electronic communication and discovers criminal conduct, release of the communication to law enforcement is permitted, giving rise to the negative implication that moni-

---

[37] Several privacy principles may be derived from the statutes: for one, the uses and limits of Title III, the Wiretap Act, as a model for serious forms of government intrusion, necessitating judicial, or at a minimum, grand jury sanction; as well as the curative effect of notice, in terms of impeding secret government files and actions. Notice to the customer may be waived under RFPA in cases where there is reason to believe that notice will result in: endangered life; flight from prosecution; destruction of evidence; intimidation of potential witnesses or serious jeopardy to the investigation or proceedings. 12 U.S.C. 3409(a).

[38] It is fairly clear that financial institutions providing wire transfer services to their customers would constitute "electronic service providers" under ECPA, in part relying on the breadth of the definition of "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system." 18 U.S.C. 2510(12). The legislative history seconds this surmise, in setting forth as an example of electronic communication, "funds transfer among financial institutions." S. Rep. No. 99-541, 99th Cong., 2nd Sess. 1, 8 (1986).

Although banks might not view themselves as "electronic service providers," ECPA would appear to, even though banks may rely upon leased telephone lines to actually conduct the electronic communications. Similarly, bulletin board services and other e-mail providers rely upon existing communication facilities, but are covered by ECPA as "electronic service providers."

[39] One of the better counterarguments to this conclusion that ECPA covers wire transfers derives from a fragment of legislative history, noting that "[c]ommon computer-to-computer communications include the transmission of financial records or funds transfers among financial institutions. . . . " S. Rep. No. 99-541, at 99th Cong., 2nd Sess. 1, 8. This might be viewed as giving rise to the shaky inference that ECPA binds only *financial institutions* providing communications services, leaving a non-financial institution such as CHIPS or the Fedwire system beyond its purview. This conclusion is not warranted, because the legislative history cited does not purport to provide a comprehensive and exclusive definition of "computer-to-computer" communications; rather it is only setting forth a non-exhaustive laundry list of modern electronic communications. In any case, *Steve Jackson Games, op. cit.,* footnote 34 , supports the proposition that acquisition of stored electronic mesengers in transit to the intended recipient violates title II of ECPA.

[40] 18 U.S.C. 2703(a) and (b).

BOX 5-3: Legal Mechanisms for Acquiring Records

- *Administrative subpoena*—exercised by executive agencies pursuant to an express grant of subpoena power for enumerated purposes; forces the production of records already maintained.
- *Grand jury subpoena*—a significant tool for criminal investigations, signed by foreman of grand jury; must be relevant and material to a matter properly before the grand jury. 18 U.S.C. 3321; Fed.R.Crim.P.6.
- *Search, seizure and arrest warrants*—supported by probable cause and signed by a magistrate, as required by the Fourth Amendment.
- *Court order*—a legislative requirement, such as Title III three judge panel court orders sanctioning wiretapping.
- *Trial subpoena*—available once a defendant has been indicted by a grand jury finding probable cause that defendant committed a crime; no judicial intervention required of prosecution in obtaining further subpoenas.

SOURCE: Office of Technology Assessment, 1995.

toring of the communications for discovering criminal conduct and informing law enforcement would be illegal.[41,42]

Many commentators have extolled the virtue of moving toward coherent and synoptic legislation in the area of privacy law, and certainly wire transfer monitoring legislation would provide an opportunity to rationalize the field and perhaps avoid conflict with the growing European movement towards comprehensive data protection. For the purposes of enabling a wire transfer monitoring system to go forward, however, revisions must be made to RFPA, ECPA, and perhaps the Privacy Act. Nevertheless, policy is poorly made fragment by fragment, a problem stemming from institutional vacuum, i.e., the United States has no centralized privacy agency which might otherwise shape a privacy agenda and provide guidance on the host of issues arising at the intersection of new technology and individual privacy.[43]

Independent of what interpretation of ECPA and RFPA will prevail, financial institutions deserve regulatory certainty, hence any monitoring proposal should clearly delimit financial institution obligations and provide safe harbor from suits. Financial institutions are properly concerned with civil suits from both the government, for failure to comply with regulatory requirements such as the BSA and suspicious transaction re-

[41] 18 U.S.C. 2702(b)(6). A similar provision is found in the contemporaneous interception provisions of Title I of ECPA (codified at 18 U.S.C. 2511(3)(b)(iv)) and permitting the disclosure of the contents of a communication if inadvertently obtained by the service provider and if pertaining to criminal conduct. See also, S.Rep. No. 99-541, 99th Cong., 2d Sess. 1, 26 ("If the provider purposefully sets out to monitor conversations to ascertain whether criminal activity has occurred, this exception would not apply" and the service provider would be criminally liable for disclosing the content of the communication).

[42] A final relevant provision states that in order to obtain a court order for information in an electronic communications system, a government agency must show that there is reason to believe the contents of the communication are relevant to a legitimate law enforcement inquiry. 18 U.S.C. 2703(d). This provision suggests how contrary to ECPA's intent this proposal would be, unless Congress deems that all wire transfer communications are relevant to law enforcement's mission.

[43] OTA has long noted the policy arguments supporting the establishment of some form of privacy ombudsman, most recently in the report *Information Security and Privacy in Network Environments*. U.S. Congress, Office of Technology Assessment, *Information Security and Privacy in Network Environments*, OTA-TCT-606 (Washington, DC: U.S. Government Printing Office, September 1994).

porting,[44] and from customers, who may sue under RFPA for improper disclosures of financial information. Consequently, a paramount consideration is the minimization of financial institution liability for complying with any wire transfer reporting requirements.

With the Annunzio-Wylie Anti-Money Laundering Act of 1992, Congress enacted a comprehensive "safe harbor," or immunity from customer suit for banks disclosing customer information under suspicion transaction reporting or other requirements.[45] While the current language is quite broad[46] it may be necessary to clarify that the safe harbor provision covers disclosures of wire transfer records where there is little or no basis for believing that a customer might be engaged in criminal conduct, or where pre-determined guidelines are followed, as in technical option 4 (see chapter 7). ECPA contains a safe harbor as well, providing that any disclosure of electronically stored communications does not give rise to civil or criminal liability, as long as the disclosure was in good faith reliance upon a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization.[47]

To minimize the intrusiveness of a wire transfer monitoring system, an administrative regime might be set up to require human confirmation of any positive "hit" before more intrusive traditional law enforcement techniques are applied. This would assure that targets misidentified by false positive hits do not have their right to seclusion unnecessarily disturbed.[48] Under such a system, a human operator would intervene and search for confirming evidence, before authorizing intensified scrutiny, as part of graduated progression of escalating surveillance. As a further protection against unwarranted intrusions into innocent conduct, the process might grant notice to the targeted party, although this notice should be carefully circumscribed to prevent tipping off malefactors. Of course, the intervention of a human operator carries negative effects, as well, raising the possibility of official misconduct and unauthorized access.[49] A priority in crafting a balanced system would be the inclusion of security safeguards to limit unauthorized browsing, as well as guidelines to limit official discretion and to protect against arbitrary and capricious action. At the same time, discretion can also operate as a safety valve, in permitting agents the latitude to terminate investigations without merit before any damage is done to innocent parties.

---

[44] 12 U.S.C. 5313(g). RFPA, at 12 U.S.C. 3413(d), specifically states that nothing in RFPA "shall authorize the withholding of financial records or information required to be reported in accordance with any Federal statute or rule promulgated thereunder." Hence, financial institutions are obligated above all to comply with government dictates, with the potential of leaving them exposed to civil liability.

[45] Pub. L. 102-550, section 1517, 106 Stat. 4059-4060, codified at 12 U.S.C. 3413(g)(3). The provision states that "[a]ny financial institution that makes a disclosure of any possible violation of law or regulation or a disclosure pursuant to this subsection or any other authority . . . shall not be liable to any person . . . for such disclosure . . . ."

[46] "Safe harbor" provisions do not deter the bringing of suits, however, a continuing source of bank concern. *See,. e.g.*, *MacLean* v. *Riggs Nat'l Bank*, (No. 94-0259-CRR, D.D.C. 1994)(plaintiff suing bank for a breach of RFPA, where plaintiff had defrauded bank and bank had reported crime to federal authorities).

[47] 18 U.S.C. 2707(d).

[48] The Supreme Court recently spoke to the issue of false positives in the computing context in *Arizona* v. *Evans*, where a computer erroneously indicated the existence an outstanding warrant on Isaac Evans, resulting in his false arrest and subsequent conviction on unrelated charges. (Docket No. 93-1660, March 1, 1995). While a 7-2 majority ruled to uphold the arrest because the police were acting in good faith reliance on the computerized records, five justices signaled their concern for the dangers of computer errors and loss of liberty. Significantly, the majority opinion relied upon the fact that judicial personnel, not law enforcement, were culpable in the computer error. Perhaps, a court will be disinclined to follow the *Evans* precedent where law enforcement itself was to blame for computerized errors.

[49] For this reason, some privacy advocates object least to a "black box" system, which would assess each wire transfer on the fly against a profile of money laundering attributes, discarding all those transfers not meeting the profile. OTA Workshop on Privacy and Confidentiality, September 28, 1994.

THE PRIVACY OF THE INDIVIDUAL AND THE CONTROL OF CRIME

> No law can ever be made but what trenches upon liberty: if it stops there, it is so much pure evil: if it is good upon the whole, it must be in virtue of something that comes after. It may be a necessary evil: but at any rate it is an evil. To make a law is to do evil that good may come. J. Bentham, *Of Laws in General*, H.L.A. Hart, ed. (London: Athlone Press, 1970), chapter VI, 4, p. 54.

Few wire transfers are initiated by individuals, in relation to the total number and dollar volume of wire transfers.[50] Consequently, commentators concerned about individual privacy in payment systems have focused on consumer transfer systems, which include automated clearing houses (ACHs), automated teller machines (ATMs), point-of-sale and other forms of electronic debiting transactions.[51] Consumer transactions contain a wide variety of information, potentially indicating individuals' spending habits, lifestyles, and locations, as well as political and religious expressions. The sort of information that may be harvested from these types of transactional records would be rather distinct from the kind of information in wire transfer records, even with respect to the natural persons using the wire transfer apparatus.[52] And while consumer transactional information may be interesting to law enforcement's control of money laundering, the proposed monitoring systems would only analyze wire transfers over wholesale payments systems.

Although the current wire transfer system is predominantly a corporate instrument, there may be momentum to individual or closely held corporate use of the wire transfer.[53] Emerging forms of electronic payment, such as digital money (see box 7-4 in chapter 7) may serve the needs of individuals for immediate payments over networks. If so, then the intrusion of a monitoring system on individuals' or even corporations' privacy would be slightly mitigated by the existence of a more secure and equally efficient alternative. But this line of analysis may be begging the question, if the monitoring of funds transfers serves as a precedent for government monitoring of digital money systems. The threat of the slippery slope may be somewhat overstated, however, in light of the very different character of wholesale wire transfer systems and consumer systems, the latter of which already enjoy considerable legal protections.

---

[50] Telephone interview with Ed Regan, Vice President, Chemical Bank, August 16, 1994; interview with John Byrne and Kawika Daguio, American Bankers Association, August 4, 1994. Although law enforcement would putatively be looking at corporate transactions, one of the intended results is the prosecution of individual money launderers, along with the punishment of criminally tainted corporations by revocation of charters and fining corporations to the extent of their assets. Thus, the system could potentially circumvent the panoply of procedural requirements protecting the individual. *Boyd* v. *United States* may still speak to this question, as the facts of the case are somewhat analogous, with law enforcement targeting individuals by searching corporate documents without probable cause. 116 U.S. 616 (1886) ("illegitimate and unconstitutional practices get their first footing . . . by . . . slight deviations from legal modes of procedure").

[51] These transactions are covered by the Electronic Funds Transfer Act of 1978 (EFTA)(Pub. L. 95-630), codified, as amended, at 15 U.S.C. §1693 *et seq*. EFTA, and its implementing Regulation E, which provide privacy and other protections to electronic funds transfers connected to consumer accounts, accounts "established primarily for personal, family, or household purposes." 15 U.S.C. §1693a(2). All funds transfers through Fedwire, however, "even those involving consumer accounts, are exempt from EFTA and Regulation E." E. Patrikis, T. Baxter, and R. Bhala, *Wire Transfers*: *A Guide to U.S. and International Laws Governing Funds Transfers* (Chicago, IL: Bankers Publishing Co., 1993), p. 147. An interesting thought deriving from this last statement would be that individuals already use the wholesale funds transfer system at their own peril and assume the rules of its game, including perhaps, future monitoring for money laundering.

[52] The American Bankers Association demurs slightly, in observing that the wire transfer messages of individuals, often relating to small dollar cash transaction or investment activities, may contain highly personal information and instructions relating to specific investments and business transactions.

[53] Citicorp offers the WorldLink product, a gateway for small business use of the wire transfer system. Increasingly, big banks are able to offer on-line access to the wire transfer system to their clientele, bringing the marginal costs of wire transfers down dramatically.

Conceptualizing the Intrusion

The Initial Access Question

Marx and Reichman have argued that where the subject of a search is unaware of the search, where neither direct nor willing consent has been given to a search, the search is more intrusive.[54] This secret surveillance is believed to be particularly intrusive if the subjects are not given notice that they are a "positive hit," or thought to be suspect. Although these judgments were developed in the context of computer matching to detect fraud in entitlement programs, they might also be applicable to asset seizure, where the presumption of innocence is transformed into asset holder's affirmative duty to disprove the connection to illegal conduct.

The Subsequent Manipulation of the Data and the Problem of False "Hits"

While some argue that any secondary use of wire transfer information should be strictly controlled, a greater concern arises once a positive "hit" is generated and acted upon. At this point, the concern is one of the damage, economic or otherwise, visited upon the innocent party unjustly brought under suspicion by a false positive "hit," an occurrence that can be expected to be common for any wire transfer monitoring system.[55] Errors arising out of computer matching systems have been categorized as falling into two broad classes: 1) flaws in the computing/data entry system; and 2) flaws in attempting to reduce analysis to a rule-based system, what Marx and Reichman term the "acontextual nature" of computer reasoning. Both flaws may result in false positive "hits," although the first group should become progressively smaller (but never to disappear entirely) as computing technology improves.

The first group breaks down further into erroneously reported or entered data; obsolescence of information from initial entry; and computer hardware/software errors. The latter group has been identified by Marx and Reichman to be the "acontextual nature of the decision process, and the probabilistic nature of profiling" (i.e., coincidences of profiling). The latter errors would be expected to arise repeatedly when a profile is used to separate licit and illicit wire transfers on the basis of the sketchy information contained in the wire transfer. For instance, threshold clearing accounts, described in chapter 1, are a standard business practice, yet also resemble money laundering schemes. Also, the profiles are likely to be skeletal, hence many innocent people can be expected to meet the profile by pure coincidence. Additionally, law enforcement has no baseline figures for what the proper ratio of positive to negative should be, nor, in fact, can law enforcement be certain that all money laundering schemes are incorporated into the profile—knowledge is distorted by the detected criminals, who are ipso facto less competent than their unapprehended money laundering cohorts.

What are the costs to targets falsely labeled as suspicious? Presumably, investigations will intensify, with intrusive, albeit legal tools of modern law enforcement. One could expect that businesses, in particular, could suffer deleterious economic consequences should the law enforcement

---

[54] Gary T. Marx and Nancy Reichman., "Routinizing the Discovery of Secrets," *American Behavioral Scientist*, (March/April 1984), pp. 423-52, 440. But disclosure of a search may often vitiate the law enforcement mission: consider the U.S. Customs Service's practice of having dogs sniff international luggage in transit before passengers claim their bag. Otherwise, if a dog "alerts" to narcotics in a bag, the narcotics trafficker would be expected to abandon the bag, leaving the agents with the contraband but not the miscreant.

At least one expert from the law enforcement community disagrees with the proposition that undisclosed non-retained screening compromises privacy. Telephone interview with Scott Charney, Chief, Computer Crime Unit, Department of Justice. Consider also the aforementioned case of *Steve Jackson Games* and the constitutional obligation to avoid the seizure and review of the contents of communications not relevant to a law enforcement inquiry. 36 F.3d at 463. The court observed that computerized key word searches of unread e-mail to filter out irrelevant or innocuous messages decreased the risk of improper access to innocuous communications.

[55] See chapter 4, box 4-5, for a fuller discussion of the problem of false positive in settings with low incidence of the conduct being sought.

scrutiny become public.[56] A further detriment to the computer "hit" could be a shift in the presumption of guilt, in the sense that a computer can precipitate the seizure of assets.[57]

Balancing the Interests of Law Enforcement and the Individual

The Changing Balance of Power Between Criminals and Law Enforcement

As criminals become increasingly sophisticated and take advantage of new technology, crime itself becomes less apparent, particularly so with "victimless" crimes such as money laundering. In the case of wire transfers, the money launderers conceal their activity in the stream of commerce. Law enforcement argues that if it may not legitimately scrutinize the electronic stream of commerce for wrongdoing, criminals will go undetected and unpunished.

Sometimes technology greatly aids law enforcement's mission, such as computerized databases available for instantaneous records checks and computerized fingerprint analysis. But at the same time, emerging technologies like public key encryption and digital telephony may undermine law enforcement efforts. Will law enforcement be permitted to shape (and perhaps pay for) the structure of technological development to keep the balance of power between law enforcement and the criminal element status quo or to tip the balance in society's favor? At the same time, technology may offer the best of both worlds, sheltering privacy while permitting increased investigative powers. This could permit anonymous payments until certain objective criteria are satisfied, established either by legislative or administrative regime and justifying access to the wire transfer.

This argument regarding the balance of power between law enforcement and the criminal may be irrelevant. The criminal is relying upon electronic technology for the execution of the crime of money laundering. This distinguishes a wire transfer monitoring system from the usual scenario, where the increased intensity of electronic surveillance would shift the balance of power between the state and the scrutinized in permitting electronic technology to manipulate data in ways that paper could not be analyzed. In a sense, criminals are benefiting from technology and exposing themselves to detection at the same time.

The Costs of Traditional Law Enforcement Techniques

What are the costs of traditional law enforcement techniques where the traditional citizen-reporting model for detecting offense is not tenable?[58] Given the near invisibility of money laundering, particularly past the placement stage, law enforcement has relied heavily upon undercover operations in trapping money launderers,[59] raising the specter of, at best, police complicity in permitting money laundering to go forward in order to build a case, with a strain on limited police resources to conduct storefront operations; or at worst, entrapment and police corruption. Consider also the French example: TracFin, the French

---

[56] If a corporation is publicly suspected of narcotics trafficking or money laundering, in all likelihood its banks will cut off banking relations lest the banks later be accused of complicity in further money laundering. Of course, many other examples of economic harm may be readily imagined—vendors demanding cash upon delivery out of a concern for future legal problems, and so on.

[57] Marx and Reichman, op cit., footnote 51, p. 441. Privacy advocates favor followups to positive hits before entitlement program benefits are cut off. "[T]o protect due process and Constitutional rights, however, this effort [to computer match and save money] should also involve detailed and, where necessary, extensive followup efforts." David F. Linowes, *Privacy in America: Is Your Private Life in the Public Eye?* (Urbana, IL: University of Illinois Press, 1989), p. 95. In all likelihood, any computer "hit" would be buttressed by independent evaluations to form reasonable suspicion before a seizure is effected.

[58] One lost asset of citizen reporting is its inherent ability to circumscribe police discretion, hence other means to control discretion must be sought out in the case of electronic surveillance. Marx and Reichman, "Routinizing Surveillance," *op. cit*, footnote 54, p. 423. See, generally, Gary T. Marx, *Undercover: Police Surveillance in America* (Berkeley, CA: University of California Press, 1988).

[59] In fact, the money laundering criminal statute had to be redrafted soon after its initial enactment to accommodate sting operations.

intelligence agency which is a near analog to the United States' FinCEN (see chapter 3), relies on a network of informants within the banks themselves to report suspicious activity by phone or fax.[60] Perhaps most interesting for the current analysis are the secrecy "agreements" that the informants enter into with TracFin, wherein they promise not to reveal their communications with TracFin to their fellow bank employees. The costs of trying to enforce money laundering statutes without recourse to computer surveillance would be an increased amount of human surveillance and spying within the banking system itself (with difficulties in limiting the scope of the human surveillance to the immediate task of ferreting out money laundering).

The Control of Government Over Society

Some commentators associate increasing social control with conformity and a loss of individuality.[61] Others counsel against the irreversible trend of systems of government towards more intensive and extensive social control. Marx notes that law enforcement, like all apparatuses of social control, tends toward increasing rationalization, in seeking to be more effective, efficient, certain and predictable.[62] Many privacy commentators have adopted and adapted Bentham's concept of the panoptic eye, originally scrutinizing the incarcerated for purposes of controlling prisons, but now turned outward regarding all citizens and their transactions with suspicion, measuring their conduct against a backdrop of criminality.[63] Some social scientists qualify this panoptic argument, stating that evidence for changed behavior in the face of perceived surveillance must be seen, before inferences of tyrannical social control may be drawn.[64]

Interestingly, the BSA reporting requirements present an example of the often paradoxical response of society to a new attempt at social control. After law enforcement's wakeup call to the banking community as well as the criminal element with Operation Greenback and the Bank of Boston case (see chapters 1 and 3), the phenomenon of smurfing arose, as money launderers sought to discover a new invisible path into the financial system. The behavior of miscreants has changed, but little is known about whether legitimate cash transactors have changed their behavior, whether government control has adversely influenced the innocent individual.

The control of crime is central to the functions of modern governments, in the maintenance of a stable social order. The sovereignty of the state may be at stake, in its inability to control money across borders and protect the integrity of its cur-

---

[60] Interview with Joseph Myers, Asst. Legal Counsel of FinCEN; TracFin's 25 agents work with about 4,000 "correspondents," one in each of financial institutions, reporting about 60 tipoffs each month. Monaco has recently set up an analogous agency, Siccfin, to follow dirty money. "Monaco acts to cut down dirty laundry," Andrew Jack, *Financial Times*, October 25, 1994, p. 2.

[61] See, e.g., Edward J. Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser," 39 *N.Y.U. L. Rev.* 962, 1003 (1964)("The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity. Such an individual merges with the mass.")

[62] Marx and Reichman, *op. cit.*, footnote 54, p. 442. Marx also observes that any dramatic shift towards a totalitarian state would likely occur "by accretion [rather] than by cataclysmic event." Marx, *Undercover*, *op. cit.*, footnote 55, p. 229. Whether wire transfer monitoring would represent a significant "accretion" would likely hinge on the legislative regime authorizing the monitoring.

[63] For instance, Oscar H. Gandy, *The Panoptic Sort: A Political Economy of Personal Information* (Boulder, CO: Westview Press, 1993). In other writing, Marx notes that "mass" surveillance violates the spirit of the Fourth amendment, "because the burden of proof is shifted from the state to the target of the surveillance," upending the traditional American tenet of innocence until proven guilty. Marx, *Undercover*, *op. cit.*, footnote 58, p. 227.

[64] See, e.g., David Lyon, *The Electronic Eye: The Rise of Surveillance Society* (Minneapolis, MN: University of Minnesota Press, 1994). Lyon casts a skeptical eye at blanket assertions that technology inevitably enhances the power of organizations over the surveyed population. p. 166.

rency. The state's decision regarding what to criminalize lies at the heart of sovereignty, a decision increasingly undermined by the impunity with which the money launderer moves money across international borders.

Unanticipated Consequences of a Monitoring System

Many commentators note the leveling effect of computer analysis of records: in a sense, everyone's privacy is violated blindly and equally.[65] Nevertheless, law enforcement enjoys considerable discretion in deciding which leads merit further investigation, allowing discretion back into the equation. Marx and Reichman note this in stating that

> "[t]he discovery of infractions, of course, is only the first stage in the enforcement process. . . . An overabundance of cases and disinterest, or bias on the part of the enforcement agent, may result in no action being taken." page 447, footnote 13.

Of course, governmental followup to positive matches is often considered salutary, and in fact is mandated by the Computer Matching and Privacy Protection Act of 1988,[66] though this comes in the context of required corroboration before government benefits may be cut off on the basis of a positive hit.

At the same time commentators frequently note that all the repercussions of new computer systems may not be readily and accurately anticipated. Burnham, in his influential *The Rise of the Computer State*, details repeated instances of computer systems being used for purposes quite different than their architects planned.[67] A recent example of this would be the video surveillance of public squares in English towns: instead of helping in the apprehension of violent criminals, the human monitors of the video cameras have come to observe and report parking meter scofflaws and litterers. David Lyon interprets Burnham's views even more darkly: Lyon suggests that new computer technologies augment themselves beyond the direct control of anyone.[68]

Perhaps most speculatively, the deleterious impact of the "electronic informant" on the legal system may be raised. At least one commentator, a former federal prosecutor, has questioned the uncritical receptiveness of lawyers and judges to computer evidence, a confidence he feels is misplaced, in advocating increased scrutiny of computer-generated evidence and testimony at trial. Other commentators have extolled the benefits, including uniformity, of aiding the magistrate in her determination of probable cause for search and arrest warrants, through the use of expert systems.[69]

---

[65] Both García and Marx and Reichman observe this, particularly when compared to the biases inherent in citizen reporting as the sole means for identifying suspects. Robert García, "'Garbage In, Gospel Out': Criminal Discovery, Computer Reliability and the Constitution," 38 U.C.L.A. L. Rev. 1043-1145 (1991); Marx and Reichman, *op. cit.*, footnote 54, p. 442. Consider also *Sitz*, and the emerging theory that the Fourth Amendment only guards against arbitrary distinctions in the level of scrutiny and surveillance rather than providing an absolute floor of protection against state scrutiny.

[66] 5 U.S.C. 552a(a)(8)(B)(iii) specifically exempts law enforcement agencies from the provisions of the Computer Matching Act. The Federal Privacy Act also exempts law enforcement from many of its provisions. 5 U.S.C. 552a(j)(2). At the same time, the Privacy Act's section 552a(o) governs the transfer of databases from one agency to another for matching, and could potentially impact a non-law enforcement agency's downloading information to FinCEN.

[67] David Burnham, *The Rise of the Computer State* (New York, NY: Random House, 1983).

[68] Lyon, *op. cit.*, footnote 64, p. 11.

[69] Christopher J. Moran, "A Neat Set of Legal Rules: Improving the Search Warrant Decisionmaking Process Through Guideline Implementation," submitted to Professor Henry H. Perritt, Jr., Villanova University School of Law (May 11, 1992). Available on the World Wide Web (July 19, 1995) at: gopher://ming.law.vill.edu:70/00/.ftp/pub/law/search.warrant/.files/Search.Warrant.txt

THE CONFIDENTIALITY INTEREST OF THE CORPORATION

A Short Legal History of the Corporation in America

In the early years of the United States, legislatures granted charters to corporations so that they might serve a public purpose in exchange for a monopoly right, ordinarily, the right to operate a turnpike or bridge, thus encouraging development in a capital-poor environment. This relationship of the legislature and corporation led to Justice Marshall's famous language in *Trustees of Dartmouth College* v. *Woodward*, where he observed that the corporation is "an artificial being, existing solely in contemplation of state law."[70] Nuances aside (such as the fact that corporations are created pursuant to state law and would be regulated by federal law for present purposes), the "artificial being" theory places few, if any, restrictions upon governmental actions affecting the corporation, implying that the corporate interest in confidential payments may be subordinated to the state's interest in policing money laundering.

Defenders of corporations argue that this theory is flawed, in light of the dramatic changes in the process of incorporation, as well as the ability to shop among the states for advantageous incorporation laws and the greatly reduced mandatory requirements for incorporation. They submit that the contractual theory of the nature of corporations, namely the use of contracts to minimize the problems associated with the separation of ownership and control in the modern corporation, has risen to the fore, rendering misplaced judicial and legislative reliance on vestiges of the "artificial being" theory.[71] Butler and Ribstein argue that government regulation should not interfere with the set of contractual relationships that constitute the modern corporation; however, it is unclear how far this argument may extend in the context of law enforcement. In this limited context, the presumption in favor of the state's interest in preserving law and order by detecting and punishing money laundering may permit regulation in the form of mandated disclosure of hitherto confidential payments information.

Although the *Lochner*-era and *Slaughterhouse* cases—the high-water mark of the corporation's successful invocation of the Constitution to nullify legislative regulation—ended in 1937, the modern Supreme Court has gradually, if haltingly, enhanced the corporation's status under the Constitution, even though the Constitution makes no mention of the corporation, only persons. [72] The nadir of corporate rights is represented by the *Morton Salt* decision, a late revival of the "artificial entity" theory, rejecting a corporate right to privacy.[73] While denying the general principle of corporate personhood, the Court noted that corporations "may and should have protection from unlawful demands made in the name of public investigation." Nevertheless, the Court upheld the Federal Trade Commission's access to corporate records, citing to an earlier case, where the gov-

---

[70] 17 U.S. (4 Wheat.) 518, 636 (1819). *United States* v. *Morton Salt Corp*, 338 U.S. 632 (1950), represents a late revival of the "artificial entity" theory.

[71] See, e.g., Henry N. Butler and Larry E. Ribstein, *The Corporation and the Constitution* (Washington, DC: The AEI Press, 1995), pp. ix - x, 18-22. One of the linchpins of this argument is the fact that corporations are no longer chartered by legislatures, rather incorporated by "perfunctory" state filings. Even if this historical shift in the manner of incorporation is regarded as dispositive, it is not apposite for the matter of banks, which continue to receive ornate charters specifying obligations and waivers of rights. As a result, the bank itself would be infirm in arguing that it deserves relief from the law enforcement regulations integral to the monitoring of wire transfers.

[72] Specifically, corporations invoked the protections of the 14th amendment to nullify early state health and safety regulation of the corporation.

[73] *United States* v. *Morton Salt Corp.*, 338 U.S. 632 (1950).

ernment was allowed to rummage through corporate documents on no more than an "official's curiosity."[74]

In the wake of *Morton Salt* the Supreme Court has by fits and starts extended the protections of the Bill of Rights to corporations, rendering the Constitution "a potent shield against government regulation."[75] For instance, the Court has recognized the corporation's right to invoke a limited measure of First Amendment protection for its advertising.[76] The landmark case of *First National Bank of Boston* v. *Bellotti* extended the right of political speech to corporations, although later rulings of the Court have softened *Bellotti* somewhat. [77]

Most relevant to the proposed monitoring system, the Supreme Court has extended weakened Fourth Amendment protections to the corporation. *Marshall* v. *Barlow's Inc.* struck down as unconstitutional a provision of the Occupation Safety and Health Act authorizing warrantless workplace inspections. This ruling brought some of the protections of the Fourth Amendment to commercial buildings, beyond the core Fourth Amendment solicitude for the home as castle.[78] One commentator theorizes that the decision "represented the protection of New Property—information about workplace operations that the corporation sought to conceal from government—and it demonstrated the importance of the intangible Bill of Rights [of association, privacy and speech] in the modern political economy."[79] *Morton Salt* itself cautioned against "fishing expeditions," or government searches of ordinary business records to detect illegitimate conduct,

---

[74] The Court noted that "even if one were to regard the request for information [a complete set of terms and prices for products] as caused by nothing more than official curiosity, nevertheless law-enforcing agencies have a legitimate right to satisfy themselves that corporate behavior is consistent with law and public interest." 338 U.S. at 652. The Court went on to note, however, that "[o]f course, a governmental investigation into corporate matters may be of such a sweeping nature and so unrelated to the matter properly under inquiry as to exceed the investigatory power." (citation omitted.)

[75] Carl J. Mayer, "Personalizing the Impersonal: Corporations and the Bill of Rights," 41 *Hastings L. Rev.* 577-667, p. 661 (March 1990). Mayer catalogs successful corporate invocations of the Bill of Rights—First Amendment guarantees of political speech, commercial speech, and negative free speech rights; Fourth Amendment safeguards against unreasonable regulatory and other searches; Fifth Amendment double jeopardy and liberty rights; and Sixth Amendment entitlement to jury trial. *Ibid*., appendix I, pp. 664-65. Corporations have met with success in advancing Eighth Amendment arguments as well, particularly the excessive fines clause.

[76] *Pittsburgh Press Co.* v. *Human Relations Commission*, 413 U.S. 376 (1973)("commercial speech" or advertising receiving diminished protection relative to individuals' speech).

[77] No ideology possesses a monopoly on the charter theory of the corporation: Justice Rehnquist, in dissenting on *Bellotti*, cleaved to the *Dartmouth College* theory of the corporation, in noting that a corporation "possesses only those properties which the charter of creation confers on it, either expressly, or as incidental to its very existence." 435 U.S. 765, 823 (Rehnquist, J., dissenting), quoting *Dartmouth College*, 17 U.S. (4 Wheat.) at 636. Another dissenter, Justice White, makes the interesting point that a corporation should enjoy First Amendment protections only where it furthers self-expression by the shareholders. *Bellotti*, at 805. See also, Butler and Ribstein, *The Corporation and the Constitution*, *op. cit.*, footnote 71, pp. 61-2.

[78] *See* v. *City of Seattle* also granted commercial premises Fourth Amendment protection, although the administrative warrant required will be measured not against probable cause that a violation has occurred, but rather against "a flexible standard of reasonableness that takes into account the public need for effective enforcement of the particular regulation involved." 387 U.S. 541, 545 (1967); see also *Camara* v. *City of Seattle*, 387 U.S. 523, 534-39 (1967)(adminstrative warrants must be reasonable and tightly tied to a legitimate government purpose, but need not be based on probable cause that a particular building is in violation of fire code regulations). The *See* Court also noted other cases where the Supreme Court refused to uphold criminal investigative searches violative of the Fourth Amendment simply because the illegal searches occurred on commercial rather than residential premises. 387 U.S. at 543.

[79] Mayer, "Bill of Rights," *op. cit.*, footnote 73, p. 609. Mayer goes on to question the merits of according intangible rights to a non-person, particularly under the Fourth Amendment with its embedded privacy right. *Ibid.*, p. 643-45. Mayer does not contest the propriety of according constitutional protection to corporate *property.*

but later cases have upheld very broad subpoenas.[80]

The more recent companion cases of *Ciraolo*[81] and *Dow Chemical*[82] turned on the same Fourth Amendment issue—whether aerial overflights of defendants' property constituted "searches" requiring probable cause and warrant—using identical analyses, despite the fact that the target of the overflight in one case was a natural person's backyard and the other a corporation's industrial plant. One might infer from these cases, decided on the same day, that the Fourth Amendment is now blind to the distinction between artificial and natural persons. In fact *Dow Chemical* is noteworthy for the absence of a discussion of the status of corporate entities under the Fourth Amendment.

What Is The Basis for a Corporation's Right to Confidentiality?

Judge Posner would accord the corporation a stronger privacy right than the individual. Posner is concerned that threats to the confidentiality of business information will erode the profit incentive informing entrepreneurial risk-taking. Noam and Greenawalt corroborate this view from a different perspective: they note that "arguments for confidentiality by business organizations must be cast in terms of the functioning of social institutions, and most of the arguments rest on assumptions about economic efficiency."[83] If the utility of corporate confidentiality is the overriding policy concern, then the analysis must devolve into the question of the legitimate needs of corporate confidentiality in payment systems information.

Others might argue that the rights of the corporation might emanate from the collective rights of the underlying individuals. This libertarian concern grows where the artificial entity is a closely held corporation or small partnership. Support for this viewpoint is supplied by RFPA, in its protection of corporations and partnerships with fewer than five members: as the size of corporation diminishes, the identities of those comprising it become more transparent and their *privacy* interests as members of the corporation or partnership swell. Professor Anita Allen suggests other bases for according corporations privacy rights: "the moral status of the corporation as a social participant [*i.e.*, society imposes burdens on the corporation such as taxation, liability for injuries and losses caused] demands that its 'equivalent injuries' [loss of privacy] be compensable; and that social justice demands the fullest protection of corporate privacy no less than of individual privacy."[84] This moral ground for a right to corporate privacy is at least partially undercut by Milton Friedman's seminal "The Social Responsibility of Business is To Increase its Profits,"[85] which maintains that the corporation does not bear responsibi-

---

[80] *Morton* Salt, 338 U.S. at 642; Eli Noam and Kent Greenawalt, "Confidentiality Claims: Glittering Illusions or Legitimate Concerns?" *Business Disclosure: Government's Need to Know*, Harvey J. Goldschmid (ed.)(New York, NY: McGraw-Hill, 1979), pp. 378-418, p. 387, *citing Federal Trade Commission* v. *Crafts*, 355 U.S. 9 (1957) and *Civil Aeronautics Board* v. *Hermann*, 353 U.S. 322 (1957).

[81] *California v. Ciraolo*, 476 U.S. 207 (1986).

[82] *Dow Chemical Co.* v. *U nited States*, 476 U.S. 226 (1986).

[83] Noam and Greenawalt, "Confidentiality Claims," *op. cit.*, footnote 80, p. 382-83. Economic efficiency parses as questions subject to empirical study, such as "will an industry be made less or more competitive?" "[w]ill the burden of producing the information outweigh the likely benefits of its being produced?" "[i]f the overall 'economic' effect of disclosure of the information is likely to be negative, does some other justification. . .support its being revealed?"

[84] Allen, "Corporate Privacy Rights," *op. cit.*, footnote 12, p. 638. Mayer makes the opposite point, that the corporation benefits too much from the current legal structure—on one hand endowed with limited liability for some industrial accidents, the use of voluntary bankruptcy and perpetual life, "creating unaccountable Frankensteins that have superhuman powers but are nonetheless constitutionally shielded from much actual and potential law enforcement. . .." Mayer, "Bill of Rights," *op. cit.*, footnote 73, pp. 658-59.

[85] Milton Friedman, "The Social Responsibility of Business Is To Increase its Profits," *Business Ethics: Corporate Values and Society*, Milton Snoeyenbos, Robert Almeder and James Humber (eds.)(Buffalo, NY: Prometheus Books, 1983), pp. 73-79.

lities to society other than a duty to maximize the shareholders' stake in the corporation. Vietnam-era shareholder lawsuits seeking to inform corporate decisionmaking with values other than profit maximizing met with a similar judicial conclusion.

The Subjective Expectation of Confidentiality in Corporate Communications

Corporations often negotiate separate confidentiality accords with banks conducting wire transfers on their behalf.[86] A Chicago-based Citibank subsidiary providing wire transfer services to small businesses relates how some corporate clients require them to sign confidentiality riders barring release of the information contained in wire transfers, even though their standard service agreement already contains nondisclosure clauses. Other corporations may not, relying perhaps upon an implied right of confidentiality in the customer/bank relationship[87] or simply expecting confidentiality due to the longstanding tradition of banks to maintain customer confidences.[88]

There are considerable legitimate grounds for corporations to desire secrecy in wire transfers and to fear disclosure to competitors. Sensitive information would include the size and timing of payments to legal counsel, major stock transactions,[89] payroll information, identities of and prices paid to suppliers of inputs, as well as evidence of cost structure, generally. All this information could be derived from wire transfer records, particularly because corporations, already paying a flat fee for the wire transfer service, may use empty fields within the wire transfer messages to communicate additional information.[90] If this information is useful to law enforcement, there might be information in the stream of payments similarly valuable to aggressive competitors, industrial spies and would-be defrauders of the corporation[91] (see box 5-4). At the same time, the same paucity of information on the wire transfer record that threatens the utility of any monitoring proposal (see, in particular, chapter 4)

---

[86] Vicki Roberts, Treasurer, Centex Corporation, Houston, Texas, at OTA Workshop on Privacy and Confidentiality in Payment Systems, September 28, 1994.

[87] Fischer, *The Law of Financial Privacy, op. cit.*, footnote 15, ¶7.04. The state of New York adopted this doctrine in *M.L. Stewart & Co.* v. *Marcus*, 207 N.Y.S. 685, 691 (Sup.Ct. 1924), *aff'd* 228 N.Y.S. 856 (1927). While the implied duty or contract is fairly well settled in the United States, the scope of the duty has not been fully resolved as to whether the duty of confidentiality extends beyond the depositor relationship. p. 7-15.

[88] An absolute trust in banks might not be well-placed: while banks plead the customer's expectation of privacy in the banking relationship, banks "may claim a qualified privilege against further lawsuit [defeating a privacy tort claim for disclosure of confidential communication] when [the banks] disclose accurate customer account information to another bank." Smith, *The Law of Privacy in a Nutshell, op. cit.*, footnote 13, citing *Graney Development Corp.* v. *Taksen*, 92 Misc.2d 764, 400 N.Y.S.2d 717, *aff'd* 411 N.Y.S.2d 756 (1978).

[89] Note the parallel to early wiretaps on telegraph lines, executed by parties attempting to eavesdrop upon stock tips and other sources of financial information.

This example suggests another analogy for wire transfer monitoring, the self-regulatory organizations (SROs) and their surveillance of stock exchange members for insider trading. The New York Stock Exchange uses computer systems to monitor stock traffic for evidence of insider trading and to ferret out violators. The NYSE avoids directly piercing investor confidentiality by only accessing trading records once a market perturbation is otherwise detected, for instance, from volatile stock prices around the time of public disclosure of information material to the corporation's finances. Telephone Interview with Agnes Gautier, Vice President, New York Stock Exchange, Market Surveillance Division, March 28, 1995. For this reason, this market surveillance is not directly analogous to the monitoring of wire transfer traffic.

[90] Vicki Roberts, OTA Workshop, September 28, 1994.

[91] But the counterargument would run that industrial espionage is more easily achieved by using human contacts within corporations, that the huge amount of data comprising wire transfer traffic precludes unauthorized eyes from discerning anything interesting. Based on telephone interview with Donn Parker, SRI International.

BOX 5-4: Telegraph and Early Wiretapping of Electronic Communications

In the middle of the 19th century, the invention of the telegraph was soon followed by law enforcement and national security wiretapping, a vigorous policy debate over the sanctity of telegraphic communications, and legislative compromises modeled in part upon the protections extended to an analogous form of communication, the mails. Several similarities to the present issue bear mention: for one, the telegraph network of the United States was in its infancy when the first wiretaps occurred. Moreover, the federal searches reached all telegraphs indiscriminately: no individual level of suspicion justified the search, as the telegraph companies were simply required to produce all outgoing telegram messages. Later, state laws often distinguished between the clerk's copy of the outgoing or incoming telegram and the message in transit: the clerk's copies were given less protection than the communication in transit. And finally, just as banks argue today, telegraphic service providers pleaded the trust lodged in them by their customers, who expected confidentiality in telegraphic communications.

SOURCE: David J. Seipp, *The Right to Privacy in American History* (Cambridge, MA: Harvard University, 1978).

greatly limits the capacity for abuse by competitors and others.

Congressional and Judicial Solicitude for Corporate Confidentiality: Avoiding Economic Costs for Legitimate Participants in Funds Transfer Systems

The purposes of the following discussion of the common law and statutory protections for corporate confidential information are twofold: first, to underscore that corporations' subjective desire for confidentiality is recognized as reasonable, and second, to ask whether there are sufficient protections already on the books to guard against seepage of sensitive corporate information derived from wire transfer data beyond the authorized government use. In structure this problem is not new: in a wide variety of contexts confidential business information must be disclosed to the federal government.[92]

Congress has addressed this issue and legislated to protect confidential corporation information and communications. With the Trade Secrets Act, Congress criminalized a government official's unauthorized disclosure of confidential corporate information obtained in the course of the regulatory relationship.[93] Moreover, this provision protects information beyond intellectual property and trade secrets to include a wide variety of business information, including profit and loss figures.[94] Also, the Freedom of Information Act (FOIA) exemption (b)(4) accords broad scope to the sort of confidential business information ("reverse FOIA") that cannot be released to parties requesting information pursuant to the Freedom of Information Act.[95] As further protection for

[92] Examples include the Federal Insecticide, Fungicide, and Rodenticide Act, codified at 7 U.S.C. 136h and the Toxic Substances Control Act, 15 U.S.C. 2613.

[93] 18 U.S.C. 1905.

[94] In the past, Fedwire has demurred at supplying wire transfer records out of a fear of violating the Trade Secrects Act: the information in a wire transfer record has been construed as falling under the protections of the act.

[95] 5 U.S.C. 552(b)(4). Courts do not accept conclusory business arguments for sensitivity of information, however: the business "has failed to show how analysis of the data. . .would provide competitors with a profile of exactly how a defense contractor conducts its business. . ..[disclosure of the subcontracting amounts] reveals little of the factors involved in deriving those numbers, and therefore is unlikely to work a substantial harm on the competitive positions of defense contractors." *GC Micro Corp.* v. *Defense Logistics Agency* (9th Cir. August 26, 1994)(Docket No. 92-15646)(rejecting the business claim that this data would provide competitors with a roadmap of the corporations' subcontracting plans and strategies).

sensitive information in the government's domain, Congress has made it a crime for a person knowingly to access information in federal computers without authorization or to access more information than authorized for that person.[96]

Alongside congressional recognition of corporate confidentiality, the courts have long recognized and protected sensitive commercial information. See, *Witkop & Holmes Co.* v. *Boyce*, 61 Misc. 126, 112 N.Y.S. 874 (1908):

> The names of the customers of a business concern whose trade and patronage have been secured by years of business effort and advertising, and the expenditure of time and money, constituting a part of the good will of a business which enterprise and foresight have built up, should be deemed just as sacred and entitled to the same protection as a secret of compounding some article of manufacture and commerce.[97]

Also, courts invoke "corporate privacy" routinely when limiting overbroad discovery requests in civil litigation. See, e.g., *GRET Corp.* v. *Shell Oil*, 138 F.R.D. 530 (1991).

Tavoulareas is noteworthy for its enunciation of a constitutional right of corporate privacy, limited as compared to the privacy rights of the individual[98] but more powerful than the public's First Amendment right to read published accounts of discovered material not used at trial. Significantly, both *Tavoulareas* and *Witkop* consider the value of customer names to the corporations a protected category of information and sought to protect against competitive harm.

The Economic Costs of Surveillance of Legitimate Actors

Legislative and judicial protection of confidential corporate information both supports and undercuts a claim of confidentiality, however. On one hand, it signals that such information is respected by the federal government as privileged and dangerous if publicly distributed, and recognizes that the economic impact upon the violated business is grave enough to bring criminal penalties to bear against federal officials, who might otherwise be suborned by interested parties into releasing the sensitive information. On the other hand, the criminalization of the disclosure might allay the concerns of the corporation: with criminal sanctions in place for official misconduct, the question becomes what harm is there in having the government apprised of the details of wire transfers of law-abiding businesses?

In light of the fact that experts have suggested little ground other than utility for finding a right to corporate confidentiality, the debate about government access to wire transfer data would revolve around the feasibility and costs of minimizing the possibility of a damaging leak of

---

[96] 18 U.S.C. 1030(a). The several states have also sought to protected computerized information from unauthorized access. For example, the State of New York has criminalized a variety of computer intrusions, e.g. unauthorized use of a computer, computer trespass, computer tampering and the unlawful duplication of computer related material. New York Penal Law 156.05, .10, .20, .25, .26, .27 and .30.

[97] Quoted in *Tavoulareas* v. *The Washington Post Company*, 724 F.2d 1010 (D.C.Cir. 1984), *vacated* and *remanded*, 737 F.2d 1170 D.C. Cir. 1984).

[98] Even the natural person enjoys no constitutional right to informational privacy. *Paul* v. *Davis*, 424 U.S. 693 (1976)(holding that there was no constitutional basis for limits on disclosure of arrest records—they did not concern private conduct). But see *United States Department of Justice* v. *Reporters Committee for Freedom of the Press*, where the Supreme Court held that a clear privacy interest existed in a computerized compilation of an individual's criminal record. It appears that the computerized nature of the recordkeeping environment forced the Court to deviate from the *Paul* v. *Davis* precedent, a concern which recently rematerialized in *Arizona* v. *Evans*, *op. cit.*, footnote 48 (especially O'Connor's concurring opinion observing that "[w]ith the benefits of more efficient [computer-based recordkeeping systems] law enforcement mechanisms comes the burden of corresponding constitutional responsibilities.").

information beyond the confines of the federal government.[99] That is, as the corporation cannot claim psychological damage from the unexpected disclosure of "private" thoughts or facts, the sole, but vital, basis for corporate grievance is economic: can a competitor's derivative use of the payments systems information impair the corporation's bottom line?[100] Can the government exert sufficient bureaucratic control over employees to prevent leakage and can security systems be installed to minimize the possibility of unauthorized access by employees and "crackers" alike?

The pertinent question becomes whether there are any models available for protecting information against unauthorized access. A recent OTA report, *Information Security and Privacy in Network Environments*, suggests that information security is rarely assured in the federal government, and in fact, many factors militate against guarantees of absolute security.[101] Nonetheless, the Census Bureau has a deep tradition of guarding against security breaches in its data and suggests a possible model. Currently, FinCEN utilizes access control and passwords, and has the potential for access monitoring to its Financial AI System (FAIS). But FinCEN does not use keystroke-monitoring to safeguard against unauthorized browsing in its FAIS, on the grounds that they trust their small cadre of five BSA analysts and that FinCEN lacks the computing capacity to install a monitoring apparatus atop the FAIS.[102] On the other hand, FinCEN keystroke monitors the Project Gateway access of state and local law enforcement, to deter and detect unauthorized access to CTR information. FinCEN also access monitors the more than one hundred authorized users of the IRS and Treasury Enforcement Communications System (TECS), both of which provide access to BSA data (see also chapter 3).[103] Experts within the banking community have opined that security systems in place at money center banks forestall bank employee abuse of the information contained in the wire transfer records, so it may be assumed that similar safeguards may be put in place at any central repository of wire transfer records.[104]

Recently a set of authors has proposed a solution for a similar problem of protecting sensitive business information in the very different context of permitting onsite inspections of chemical

---

[99] While this is a simple issue to formulate, the answer is elusive. The history of the Internal Revenue Service (IRS) is instructive in this regard: while more than twenty years ago the Nixon Administration abused confidential taxpayer information held by the IRS, lately, new, more mundane invasions of privacy have taken the form of numerous IRS employees browsing through taxpayer records, presumably at the behest of interested and paying parties. Other instances of government employees, such as Social Security Administration clerks, browsing through records to satisfy curiosity about celebrities, and their own acquaintances abound. See generally, Office of Technology Assessment, *Information Security and Privacy in Network Environments, op. cit.*, footnote 43, pp. 2-3, and 58 (setting forth instances of unauthorized browsing as well as some of the factors rendering ironclad security problematic).

[100] Perhaps a corporation could rely upon *Bellotti* and its confirmation of the corporation's right to speak politically for the argument that premature disclosure of political thoughts would prejudice a corporation's right to deliberate and speak politically, however, given the very limited and almost utterly nonpolitical nature of wire transfer information, this argument would stretch credulity.

[101] The General Accounting Office (GAO) has identified employee browsing through the National Crime Information Center as well as the IRS: employees have browsed records relating to friends, family, neighbors and celebrities. Office of Technology Assessment, *Information Security and Privacy in Network Environments, op. cit.*, footnote 43, pp. 2-3.

[102] Interview with Ted Senator, Chief, Artificial Intelligence Division, FinCEN, August 25, 1994.

[103] The GAO noted that more than 270,000 queries of the BSA database and 66,000 separate sessions took place in an eighteen month period ending June 30, 1993. This volume of queries would be a challenge to keystroke monitoring. U.S. Congress, General Accounting Office, *Money Laundering: Progress Report on Treasury's Financial Crimes Enforcement Network*, (U.S. Government Printing Office: Washington, DC November 1993).

[104] But it is unlikely that financial institutions would fully disclose security breaches lest their customers seek out financial institutions with better information security.

weapons production facilities to verify compliance with the Chemical Weapons Convention.[105] Chemical weapons manufacturers fear that international inspectors will reveal trade secrets and other proprietary business information following comprehensive onsite inspections and data collection from chemical weapons manufacturers.[106] The Chemical Weapons Convention contains a variety of familiar provisions to control data leakage, including requirements for secure storage, coded identification of manufacturing facilities, as well as nondisclosure agreements. Nonetheless, the United States may not sign the treaty, due in part to industry concerns about loss of confidential business information. Among other proposals for assuaging industry concerns, Tanzman et al. propose alternative remedies beyond those of the Trade Secrets Act. It is proposed to allow the Tucker Act to confer jurisdiction to sue the United States for compensation for the loss of confidential business information.[107] Independent of the precise limits of "takings" analysis suggested by *Ruckelshaus* v. *Monsanto*[108] (and whether, in fact, a "taking" could occur in the context of wire transfer reporting), Congress could specify a statutory compensation regime for economic harm resulting from unauthorized access to wire transfer information within the government's control. In order to minimize litigation costs, standards for evidence could be specified (e.g., use of access logs and keystroke-monitoring logs as self-authenticating evidence) and alternative dispute resolution processes could be used to speed redress and minimize litigation costs.[109] This might diminish the problems of causality—the link between the government holding of the wire transfer records and the economic harm—an especially crucial concern where other parties are privy to the wire transfer data, including originating, beneficiary and intermediary banks, as well as the originator and beneficiaries themselves. Nevertheless, the waiver of sovereign immunity, or consent to be sued for loss of confidential business information, would impose a salutary incentive on agencies in possession of the confidential wire transfer records, particularly if any damages claims were required to come out of the agencies' general appropriations.

CONCLUSIONS

This chapter has set forth many of the concerns that would plague the indiscriminate monitoring of wire transfer traffic. More finely detailed assessment of the costs of the various technological configurations as well as necessary statutory changes are spelled out in Chapter 7. As a general matter, however, facilitating the technological configurations would further underscore the unsettled and "patchwork" nature of "data protection" in the United States, requiring a roll-back in existing privacy protections. A further complica-

---

[105] Barry Kellman, David S. Gualtieri and Edward A. Tanzman, "Disarmament and Disclosure: How Arms Control Verification Can Proceed Without Threatening Confidential Business Information," 36 *Harvard J. Intl. Law* 71-126 (Winter 1995), citing the *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, opened for signature* January 13, 1993, 32 *I.L.M.* 800 (not in force).

[106] *Ibid*. at 74.

[107] The Tucker Act is codified at 28 U.S.C. 1491(a)(1).

[108] 467 U.S. 986 (1984). *Monsanto* is noteworthy in several respects. First, intangible proprietary information is recognized as "property" protected by the Fifth Amendment. Furthermore, the Court observed that government could "take" property, prompting a claim for just compensation, even if government did not acquire or destroy the property. A mere interference with reasonable investment-backed expectations can cause a "taking" under the Fifth Amendment. In the wire transfer context, the argument remains to be made that the mere reporting of wire transfers would interfere with investment-backed expectations. In *Monsanto*, the Court considered the legislatively mandated sharing and sale of proprietary data to competitors to be possible "takings."

[109] Cf. Tanzman *et al., op cit.*, footnote 105, pp. 122-124. This proposal would raise budgetary issues—at what weight would this contingent liability be assessed by the Congressional Budget Office?

tion stems from the fact that European countries are moving toward a uniform regime protecting data against secondary use not consistent with the purpose for which it was collected.[110] Any monitoring proposal runs contrary to this fundamental precept of European data protection and fair information practices.

As noted in the preceding discussion, however, there is a long tradition of assessing "privacy" concerns from the perspective of the Fourth Amendment and the Constitution in this country, a tradition that might suggest that the overlaying of fair information practices or "data protection" is unnecessary or inapposite for deciding questions of law enforcement access to information. Several arguments drawn from American legal thought undercut the claim that wire transfers might have for freedom from law enforcement access. Transactions within the stream of commerce receive diminished protection under the Bill of Rights. Moreover, the kind of information in a wire transfer is at a considerable remove from the core concerns of the Fourth Amendment, political thought and the sanctity of the home.

Yet, confidentiality in business communications still looms as a large concern, although this concern may be partly addressed by ensuring proper security safeguards for the wire transfer data. An extreme measure to protect the data would be a waiver of sovereign immunity, to permit corporations to sue the government for economic damages suffered. This would require Congress to pay for the privilege of endangering corporate confidential business information, impose incentives on the handlers of data to safeguard it, and hence preserve the corporation's incentive to engage in entrepreneurial conduct.

[110] The European treaties and laws on data protection, including the recently adopted European Union Data Protection Directive, are discussed at greater length in the following chapter.