"DOUBLETHINK"ING PRIVACY UNDER THE MULTI-STATE ANTITERRORISM INFORMATION EXCHANGE[1]

Thomas V. Burch[*]

"Historically, the greatest threat to personal privacy has been the State. It still is. Jealous of its own secrets, the government covets ours."[2]

TABLE OF CONTENTS

---

* B.A., B.B.A., Mississippi State University; J.D., Florida State University; Associate at King & Spalding in Atlanta. I would like to thank Beth (for everything, and then some) and Professor Steven Gey for taking the time to talk with me about this article and life in general. I couldn't have written this without either of you. As always, any errors are my own.

1 GEORGE ORWELL, 1984 82-83 (Centennial ed. 2003) (1949). "Doublethink" was the guiding principle of the Big Brother Party in George Orwell's *1984*. *Id.* Essentially, "doublethink" referred to the Party's ability to shape its followers' beliefs in a manner that defied common sense and logic. *Id.* Followers of the Party believed that if the Party said it, then it must have been true. *Id.*

> In the end the Party would announce that two and two make five, and you would have to believe it. It was inevitable that they should make that claim sooner or later: the logic of their position demanded it. Not merely the validity of experience, but the very existence of external reality was tacitly denied by their philosophy. The heresy of heresies was common sense.

Id. Matrix officials are currently applying this logic anytime someone challenges the appropriateness of the Matrix system. Robert O'Harrow, Jr., *U.S. Backs Florida's New Counterterrorism Database: "Matrix" Offers Law Agencies Faster Access to Americans' Personal Records*, WASH. POST, Aug. 6, 2003, at A1. They religiously refer to the "war on terror" in an effort to sway public opinion in favor of the program, believing that if they mention the phrase often enough, the public will begin to believe that the Matrix is a virtuous system, only aimed at ending the terrorist threat. *Id.*

2 CHARLES J. SYKES, THE END OF PRIVACY 155 (1999).

I. Introduction

James Madison believed that the great difficulty in creating a government of "men over men" lies in the following challenge: "you must first enable the government to control the governed; and in the next place oblige it to control itself."[3] Succeeding in this challenge is especially difficult during times of national crisis. As the dangers to national security increase, civil liberties decrease. The relationship is both automatic and axiomatic. However, history has not clearly defined the extent to which individual civil liberties should suffer in the face of national exigencies. How much control over the individual should the government assume in the name of national defense?

The current "war on terror" provides an apt example. In the name of national security, the government has recently instituted several law enforcement programs that pose serious threats to individual privacy. In 2002, for example, the Defense Advanced Research Projects Agency ("DARPA") created Total Information Awareness ("TIA"), a data surveillance program that the Pentagon could use to "detect, classify, and identify potential *foreign* terrorists."[4] However, DARPA designed

---

[3] THE FEDERALIST NO. 51 (Alexander Hamilton, John Jay, and James Madison).

[4] DEFENSE ADVANCED RESEARCH PROJECTS AGENCY, REPORT TO CONGRESS

the TIA to collect extensive records on all *American* citizens, regardless of whether they had ties to terrorist organizations.[5] The system contained magazine subscription lists, credit records, and – through its use of commercial databases that collect records from the internet – several other types of highly personal information.[6] When Congress learned about the true extent of the TIA program, it immediately passed a moratorium on the program's funding.[7]

Far from being deterred, however, the executive branch of the federal government responded by attempting to establish the same type of system through state cooperation. In 2003, the Justice Department and the Department of Homeland Security pledged $12 million to the Multi-State Antiterrorism Information Exchange ("Matrix"), a Florida-based program that is strikingly similar to the TIA.[8] Proponents say the

---

REGARDING THE TERRORISM INFORMATION AWARENESS PROGRAM 3 (May 20, 2003) [hereinafter DARPA REPORT] (emphasis added). The program's original name was Total Information Awareness; however, after critics began to raise privacy concerns about the TIA, the Pentagon changed the program's name from *Total* Information Awareness to *Terrorism* Information Awareness. *Id.* The name change was not successful in quelling those privacy concerns. *See* Carl Hulse, *Congress Shuts Pentagon Unit Over Privacy*, N.Y. TIMES, Sept. 26, 2003, at A20.

[5] *See* William Safire, *You are a Suspect*, N.Y. TIMES, Nov. 14, 2002, at A35.

[6] *See id.* The Pentagon planned to enter this information into what it termed a "virtual, centralized grand database." *Id.*

> Modern technology has made it possible to create vast new dossiers of extraordinary detail and specificity about our tastes, habits, and lives. Every time you apply for a job, subscribe to a magazine, call a mail-order catalog, use a credit card, dial a phone, seek credit, fly on an airplane, buy insurance, rent an apartment, drive a car, pay taxes, get married or divorced, sue someone, see a doctor, use a smart card, apply for government licenses or benefits, you become part of the dataweb, which has proven far more powerful than the paper trails of bygone years.

SYKES, *supra* note 2, at 5; *see also* Barry Steinhardt, *Liberty in the Age of Technology*, GLOBAL AGENDA, Jan. 16, 2004, at 154 (examining the need for restraints on the use of technology to protect privacy), *available at* http://www.globalagendamagazine.com/2004/barrysteinhardt.asp (last visited March 23, 2004).

[7] *See* Hulse, *supra* note 4. When Congress learned that the Pentagon, as part of the overall TIA project, was developing a terrorism futures market where traders could wager on the likelihood of terrorist events or political assassinations, it forced the Pentagon to close its Information Awareness Office within a day. *Id.*

[8] O'Harrow, Jr., *supra* note 1. One of the more striking similarities between the Matrix and the TIA is that both programs were designed by persons with criminal histories. *Id.* Admiral Poindexter, creator of the TIA, has a conviction for five felony counts of lying to Congress, obstructing a congressional inquiry, and destroying official documents. *See Total Information Awareness*, WASH. POST, Nov. 16, 2002, at A20; Safire, *supra* note 5. Likewise, Hank Asher, the founder of SeisInt, is a known drug smuggler. O'Harrow, *supra* note 1. "In 1999, the Drug Enforcement Administration and the FBI suspended information

Matrix simply allows law enforcement to share and access data that can help in the fight against terrorism.[9] Critics say the Matrix unconstitutionally invades privacy.[10] This Article examines the development of the Matrix program and analyzes its effect on what Justices Warren and Brandeis termed the individual's "right to be let alone."[11]

To understand the Matrix's effect on individual privacy, one must scrutinize the program in the context of United States history. From the Alien and Sedition Acts to the Red Squads of the 1960s and 1970s, Part II of this Article examines how civil liberties often suffer unnecessarily in times of national crisis. Part III then discusses how this truism applies in the current "war on terror" and details the development and operation of the Matrix system, along with that of its predecessor, the Pentagon's Total Information Awareness. Both programs, like the Alien and Sedition Acts and the Red Squads before, raise serious privacy concerns and deserve additional scrutiny.

Finally, Part IV recognizes that, while the government should have the surveillance power necessary to strengthen national security, any exercise of the government's surveillance power must give "regard to the public good and to the sense of the people."[12] More specifically, Part IV analyzes the Matrix in the context of the constitutional protections of the First and Fourteenth Amendments. However, realizing that these protections may not be broad enough to effectively control the Matrix program, Part IV also discusses the possibility of involving state legislatures in the privacy battle. Currently, state legislatures may be the only governmental body capable of protecting individual privacy from the executive branch's constitutional excess.[13]

---

service contracts with an earlier Asher-run company because of concerns about his past." *Id.*

9 *See* Susan Gast, *Matrix and Privacy: Debate Over Information Hits Close to Home*, ATLANTA J. CONST., Oct. 19, 2003, at F1 (statement of Gerald M. Haskins, Professor of Computer and Information Science and Engineering, University of Florida).

10 *See id.*

11 *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 194 (1890). While Thomas Cooley actually came up with the phrase "the right to be let alone," Warren and Brandeis popularized it in their 1890 article. SYKES, *supra* note 2, at 91-92.

12 THE FEDERALIST NO. 31 (Alexander Hamilton).

13 *See infra* Part IV.C.

II. The Politics of Fear

From the Alien and Sedition Acts of 1798 to the Red Squads of the 1960s and 1970s, "United States history reveals that the state and federal governments have rarely passed up the temptation offered by the 'pressing exigencies of crisis' to enlarge their power and serve ulterior motives, at the expense of constitutional rights."[14] Yet, as Justice Marshall once noted, "when we allow fundamental freedoms to be sacrificed in the name of real or perceived exigency, we invariably come to regret it."[15] The following examples of our government's past constitutional infringements place the Matrix in perspective and serve as reminders to closely scrutinize government programs like the Matrix that attempt to circumscribe constitutional liberties.

A. *Alien and Sedition Acts*

During the summer of 1798, only seven years after the ratification of the Constitution, John Adams convinced the Federalist majority in Congress to pass a sedition act, which, once enacted, would fine and imprison "any person who shall write, print, utter or publish . . . any false, scandalous and malicious writing or writings against the government of the United States."[16] Nominally passed to diminish the domestic impact of the French Revolution, the Sedition Act was actually a flawed effort by Adams to maintain control over the young Republican Party and Adams' Republican Vice President Thomas Jefferson.[17] "Under the guise of patriotic purpose and internal security,

---

[14] Nancy Murray & Sarah Wunsch, *Civil Liberties in Times of Crisis: Lessons from History*, 87 MASS. L. REV. 72, 73 (2002).

[15] Skinner v. Ry. Labor Executives Ass'n, 489 U.S. 602, 635 (1989) (Marshall, J., dissenting).

[16] William T. Mayton, *Seditious Libel and the Lost Guarantee of a Freedom of Expression*, 84 COLUM. L. REV. 91, 123 (1984) (quoting Act of July 14, 1798, ch. 74, § 2, 1 Stat. 596, 596). The Sedition Act was one of four acts passed within a four week period in July of 1798 commonly known as the Alien and Sedition Acts. Gregory Fehlings, *Storm on the Constitution: The First Deportation Law*, 10 TULSA J. COMP. & INT'L L. 63, 65 (2002). The other three were the Alien Act, the Alien Enemies Act, and the Naturalization Act. *Id.*

[17] Murray & Wunsch, *supra* note 14, at 73. Jefferson condemned the Alien and Sedition Acts in words that resonate today, given that programs like the Matrix are nominally aimed at "fighting terrorism." *Id.* According to Jefferson, "the friendless alien has indeed been selected as the safest subject of a first experiment; but the citizen will soon follow, or rather, has already followed, for already has a sedition act marked him as its prey . . . ." *Id.* at 74 (quoting the Original Draft of the Kentucky Resolution, October, 1798).

the Federalists enacted a program designed to cripple, if not destroy, the Jeffersonian party."[18] In fact, the Act purposefully protected Federalist incumbents from criticism and conveniently expired on the last day of the Adams Administration.[19]

Before the Act expired, however, the government prosecuted seventeen people, and the press considerably reduced its criticism of government officials.[20] A number of anti-Federalist newspapers even went out of business.[21] Significantly, these events encouraged a growing opposition to the Act that contributed to Thomas Jefferson's election as the next President of the United States.[22] When Jefferson took office, he pardoned everyone convicted under the Act.[23]

Yet, the long-term damage of the Act was irreversible. The Federalists claimed that the power to enact such a law was an implied right, "one of the now common 'national security' variety."[24] Thus, the Federalists set an early precedent for future governments to follow: allowing reliance on national security as a valid reason for passing

---

[18] JAMES M. SMITH, FREEDOM'S FETTERS, THE ALIEN AND SEDITION LAWS AND AMERICAN CIVIL LIBERTIES 21 (1956). The doctrine of seditious libel originated in England in 1606 when the crown prosecutor argued that the written defamation of public officials constituted a separate offense from private libel. David Jenkins, *The Sedition Act of 1798 and the Incorporation of Seditious Libel into First Amendment Jurisprudence*, 45 AM. J. LEGAL HIST. 154, 160-61 (2001). According to the crown prosecutor, such libels were more severe than their private counterparts because they potentially harmed the stability of the state. *Id.* at 161.

[19] Mayton, *supra* note 16, at 124. The only notable federal office that the Act did not cover was the Vice Presidency, which was then the office of Thomas Jefferson, a Republican. *Id.* At this point in history, the Presidential candidate with the second highest vote total became the Vice President. Murray & Wunsch, *supra* note 14, at 73.

[20] Murray & Wunsch, *supra* note 14, at 73. One of the seventeen prosecuted under the Act included a Congressman from Vermont. Jenkins, *supra* note 18, at 156.

[21] Murray & Wunsch, *supra* note 14, at 73.

[22] Jenkins, *supra* note 18, at 156. Additionally, while the Supreme Court never ruled on the Act's constitutionality, it has since recognized "a broad consensus that the Act . . . was inconsistent with the First Amendment." *See* New York Times v. Sullivan, 376 U.S. 254, 276 (1964).

[23] Murray & Wunsch, *supra* note 14, at 74. In a letter to President Adams' wife, Jefferson stated: "I discharged every person under punishment or prosecution under the sedition law, because I considered, and now consider, that law to be a nullity, as absolute and as palpable as if Congress had ordered us to fall down and worship a golden image." *See Sullivan*, 376 U.S. at 276. "The abuses inflicted under that law did not end with the Adams administration, however, for Jefferson urged retaliation against publishers of Federalist newspapers, and some were prosecuted for common-law seditious libel." Murray & Wunsch, *supra* note 14, at 74.

[24] Mayton, *supra* note 16, at 124.

legislation that tests the boundaries of the Constitution – even when the true focus of the legislation is not national security, as was the case with the Sedition Act.[25]

B. *World War I and the First Red Scare*

In 1888, Justice Samuel Freeman Miller lectured a graduating class from the University of Iowa about the growing communist threat and warned the students about socialists and leftists that "come here and form clubs and associations; they meet at night and in secluded places; they get together large quantities of deadly weapons; they drill and prepare themselves for organized warfare; they stimulate riots and invasions of the public peace; they glory in strikes."[26] Over the next thirty years, work stoppages, anarchist bombings, and political assassinations – all of which became popularly associated with what Justice Miller might call a "communist plot" – created an Anti-Red hysteria that resembles the fear of terrorism today.[27]

---

[25] *See id.* at 123-24.

> This act could have hardly been a starker instance of self-serving politics. The Federalists, following the usual rules of political oppression, had identified an enemy without, the French, with agents within, and among these domestic agents was a "seditious" press. But undoubtedly, this Federalist talk of internal enemies was not more than poor camouflage for a measure favoring incumbency.

Id.

[26] William M. Wiecek, *The Legal Foundations of Domestic Anticommunism: The Background of* Dennis v. United States, 2001 SUP. CT. REV. 375, 380-81 (citing Samuel Freeman Miller, The Conflict in This Country Between Socialism and Organized Society, Address at the University of Iowa (1888), *in* CHARLES N. GREGORY, SAMUEL FREEMAN MILLER 168 (1907)). With the exception of the last clause, Justice Miller could just as easily have been speaking about terrorists in the year 2004.

[27] *See* Murray & Wunsch, *supra* note 14, at 75-76 ("Anarchism then inspired fears similar to terrorism today."); *see also* Harlan Grant Cohen, Note, *The (Un)favorable Judgment of History: Deportation Hearings, The Palmer Raids, and the Meaning of History*, 78 N.Y.U. L. REV. 1431, 1433 (2003) (comparing the communist threat to the terrorist threat). In comparing the government's reaction to communism in the early 20th Century to the current administration's war on terrorism, Mr. Cohen cites a 1920 report from the National Popular Government League – whose members included Roscoe Pound, Felix Frankfurter, Zechariah Chafee, Jr., and Tyrell Williams – which states:

> Under the guise of a campaign for the suppression of radical activities the office of the Attorney General acting by its local agents throughout the country, and giving express instructions from Washington has committed continual illegal acts. Wholesale arrests both of aliens and citizens have been made without warrant or any process of law; men and women have been jailed and held incomunicado [sic] without access of friends or counsel; homes have been

The first Red Scare coincided with the development of the First World War.[28] With Anti-Red sentiment growing, Congress passed the Espionage Act of 1917, which criminalized interference with military recruitment.[29] Soon after, with World War I well under way, Congress passed the Sedition Act of 1918 which, like the Sedition Act of 1798, was designed to punish political dissent.[30] It did not take long for zealous prosecutors to start relying on these Acts to fill prisons with "anti-war protestors, striking workers, and immigrants believed to be

---

> entered without search-warrant and property seized and removed; other property has been wantonly destroyed; workingmen and workingwomen suspected of radical views have been shamefully abused and maltreated. Agents of the Department of Justice have been introduced into radical organizations for the purpose of informing upon their members or inciting them to activities; these agents have even been instructed from Washington to arrange meetings upon certain dates for the express object of facilitating wholesale raids and arrests. In support of these illegal acts, and to create sentiment in its favor, the Department of Justice has also constituted itself a propaganda bureau, and has sent to newspapers and magazines of this country quantities of material designed to excite public opinion against radicals, all at the expense of the government and outside the scope of the Attorney General's duties.

Id. at 1431-32 (quoting THE NAT'L POPULAR GOV'T LEAGUE, REPORT UPON THE ILLEGAL PRACTICES OF THE UNITED STATES DEPARTMENT OF JUSTICE 1-2 (1920)). According to many, the Bush Administration's USA PATRIOT ACT is accomplishing the same type of unjust objectives as the Sedition Acts of 1798 and 1918. *See, e.g.,* David Cole, *Enemy Aliens,* 54 STAN. L. REV. 953, 966-74 (2002); *see also* Will Thomas DeVries, Note, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 283 (2003) ("The [PATRIOT ACT's] overall effect . . . has had less to do with terrorism than with easing restrictions on government surveillance of digital communications.")

[28] Murray & Wunsch, *supra* note 14, at 76.

[29] Espionage Act of 1917, 18 U.S.C. § 2388 (2000). The version of the Espionage Act that President Wilson submitted to Congress provided for a $10,000 fine and ten years in jail for any person publishing information that could be useful or possibly useful to the enemy. WILLIAM H. REHNQUIST, ALL THE LAWS BUT ONE 173-74 (1998). A presidential proclamation would determine what constituted "useful" or "possibly useful." *Id.* Wilson insisted that such censorship was necessary for the public safety and that it was imperative for Congress to pass his version of the legislation. *Id.* However, the House of Representatives vetoed Wilson's version of the bill by a vote of 184 to 144. *Id.*

[30] REHNQUIST, *supra* note 29, at 173 (citing 54 CONG. REC. 95-100 (1917)). President Wilson was very active in his support of measures to suppress political dissent. *Id.* In a message to Congress on December 7, 1915, Wilson stated:

> The gravest threats against our national peace and safety have been uttered within our own borders. There are citizens of the United States, I blush to admit, born under other flags but welcomed by our generous nationalization laws to the full freedom and opportunity of America, who have poured the poison and disloyalty into the very arteries of our national life.

Id. Congress repealed the Sedition Act in 1921, only three years after it was enacted. *Id.* at 180.

dangerously radical."[31] The prosecutors received assistance in this fight from a private organization, the American Protective League (APL), which worked with the Justice Department to track internal enemies.[32] The APL had thousands of members across the country who conducted surveillance on dissidents, harassed activists, and detained people described as having "questionable" loyalty.[33] The group also raided factories, union halls, and private homes, and "arrested" approximately 40,000 people on behalf of the War Department.[34]

Even after the War ended, the strikes, riots, and political dissent, as well as the government's prosecutions of these crimes, continued.[35] To help suppress these activities, Attorney General A. Mitchell Palmer asked J. Edgar Hoover to compile a list of radicals; that list eventually grew to over 450,000 names, including future Supreme Court Justices Felix Frankfurter and Arthur Goldberg.[36] Palmer also relied on the Espionage Act of 1917 and the Sedition Act of 1918 to quell the radical left.[37] The most effective tool at Palmer's disposal, however, was the Alien Control Act of 1918, which prohibited foreigners who believed in overthrowing the U.S. government from entering the country.[38] Palmer used the Act to arrest and deport suspected radicals that were already here.[39]

---

31 Murray & Wunsch, *supra* note 14, at 76. The government prosecuted over two thousand people under the Espionage and Sedition Acts. *Id.*

32 *Id.*

33 *Id.*

34 *Id.* This is similar to how the State of Florida is currently working with a private organization, SeisInt, Inc., to develop a database containing records on the citizens of the five states participating in the Matrix program. *See* O'Harrow, *supra* note 1.

35 *See* Cohen, *supra* note 27, at 1453-56. After the war, labor unions began reasserting control over employers and the bargaining process. *Id.* In January of 1919, harbor workers, cigar makers and dressmakers in New York began to strike. *Id.* They were soon followed by rail workers in New Jersey and a general strike in Seattle. *Id.* Many of the strikes included violence, and the labor movement became further entwined with the public's notion of left-wing revolution. *Id.* at 1455-56.

36 Murray & Wunsch, *supra* note 14, at 77-79.

37 Cohen, *supra* note 27, at 1457. The government prosecuted more than two thousand people under the Espionage Act between June 30, 1917 and June 30, 1921. *Id.* More than a thousand of these prosecutions resulted in convictions. (The Sedition Act was an amendment to the Espionage Act so these figures include prosecutions under the Sedition Act as well.) REHNQUIST, *supra* note 29, at 182-83. For an example of the type of publications that could lead to prosecution and conviction under the Sedition Act, see Abrams v. United States, 40 S. Ct. 17 (1919).

38 Cohen, *supra* note 27, at 1457.

39 *Id.*

Throughout January of 1920, Palmer planned and executed a series of raids on homes, pool halls, bowling alleys, and other "leftist" meeting places in thirty-three cities across the United States.[40] Primarily targeting Russian and Eastern European immigrants, the raids resulted in over 10,000 arrests, most of which were made without warrants or probable cause.[41] Significantly, Palmer's Justice Department adopted an internal rule that simple membership in groups, such as the Union of Russian Workers or the Communist Party, qualified individuals for deportation under the Alien Control Act.[42] Relying on this internal rule, Palmer began deporting the members of communist groups that police arrested in the raids.[43] After the fact, it became apparent that most people on these membership rolls were unaware of their membership in the groups.[44] Louis Post, the Assistant Secretary of Labor, later admitted that very few of the immigrants arrested were the kind of people that Congress intended to deport under the Act.[45] Thus, Palmer and the Justice Department misused the Alien Control Act in an effort to promote national security through the deportation of suspected communists.[46]

C. *The FBI and CIA War on Communism*

Over the next fifty years, the federal government continued to establish new laws and agencies to combat perceived international threats. Under the National Security Act of 1947, Congress established the Central Intelligence Agency "as the nation's first comprehensive peacetime foreign intelligence service."[47] The objective of the CIA was

---

40 Murray & Wunsch, *supra* note 14, at 78.

41 *Id.*

42 Cohen, *supra* note 27, at 1458. Around this same time, the House of Representatives considered a bill that would have imposed the death penalty for aiding in an insurrection. *See* A Bill to Punish Offenses Against the Existence of the Government of the United States, and for Other Purposes, H.R. 11430, 66th Cong. § 2 (1920).

43 *See* Murray & Wunsch, *supra* note 14, at 78.

44 Cohen, *supra* note 27, at 1463.

45 *Id.* at 1462. Post also admitted that only forty or fifty of the thousands arrested actually supported an overthrow of the United States government. *Id.* at 1463.

46 *See id.*

47 REPORT TO THE PRESIDENT BY THE COMMISSION ON CIA ACTIVITIES WITHIN THE UNITED STATES 10 (June 1975) [hereinafter ROCKEFELLER COMMISSION REPORT], *available at* http://history-matters.com/archive/church/rockcomm/contents.htm (last visited Mar. 6, 2004). President Ford created the Rockefeller Commission to investigate whether the CIA was overstepping its intended authority. *Id. at 3.*

to provide the President with coordinated *foreign* intelligence, which the country lacked prior to Pearl Harbor.[48] Congress did not create the CIA to replace or assist the FBI in conducting *domestic* investigations.[49] Indeed, to ensure the public "that it was not establishing a secret police which would threaten the civil liberties of Americans," Congress specifically prohibited the CIA from exercising "police, subpoena, or law-enforcement powers or internal security functions."[50]

Nevertheless, shortly after its founding, the CIA began to overstep the boundaries of its intended authority.[51] Under pressure from President Johnson, CIA Director Richard Helms initiated a series of reports on American dissidence both at home and abroad.[52] One of the papers, titled "Restless Youth," included a detailed section on the demonstration tactics of American students.[53] Recognizing the impropriety of the CIA's involvement in such a study, Helms attached a memo to the President on this report, which stated:

> In an effort to round-out our discussion of this subject, we have included a section on American students. This is an area not within the charter of this Agency, so I need not emphasize how extremely sensitive this makes the paper. Should anyone learn of its existence it would prove most embarrassing for all concerned.[54]

Thus, even though Congress specifically prohibited the CIA from monitoring the domestic activities of American citizens, the CIA knowingly gathered information on American students' political dissidence.[55] Furthermore, the CIA did not limit its domestic

---

48 *Id.* at 10-11.

49 *Id.* at 11 (emphasis added).

50 *Id.*

51 *See id.* at 130-50. "The Presidential demands upon the CIA appear to have caused the Agency to forgo, to some extent, the caution with which it might otherwise have approached [domestic investigations] . . . . These White House demands . . . seem to have encouraged top CIA management to stretch and, on some occasions, to exceed the legislative restrictions." *Id.* at 131. Part of the problem stemmed from a lack of oversight. "The excessive secrecy surrounding Operation CHAOS, its isolation within the CIA, and its removal from the normal chain of command prevented any effective supervision and review of its activities by officers not directly involved in the project." *Id.*

52 *Id.* at 132. The CIA, unlike the FBI, generally produced finished, evaluated intelligence. *See id.* Presumably, this is the reason that President Johnson asked Helms, as Director of Central Intelligence, to compile a "coordinated evaluation of intelligence bearing upon the question of dissidence." *Id.*

53 ROCKEFELLER COMMISSION REPORT, *supra* note 47, at 134.

54 *Id.* at 134.

55 *Id.* at 130.

surveillance to American students alone.[56] Through a Special Operations Group commonly known as Operation CHAOS, the CIA created more than 7,200 files on citizens of varying backgrounds.[57] These files included approximately 300,000 names of persons and organizations.[58] Seventy-five of the persons were members of Congress.[59] One CIA agent even became an advisor in a United States congressional campaign and furnished reports to the CIA of behind-the-scenes campaign activities.[60]

Around this same time, the FBI also ran a series of covert operations – which it called Counter Intelligence Programs ("COINTELPROs") – aimed at suppressing movements for social change.[61] During the course of these operations, J. Edgar Hoover created files on more than 450,000 Americans.[62] However, Hoover went beyond simply collecting files to undertaking "secret action designed to 'disrupt' and 'neutralize' target groups and individuals."[63] His agency's techniques ranged from "mailing anonymous letters to a [target's] spouse accusing the target of infidelity . . . to contacting an

---

[56] *Id.*

[57] *Id.*

[58] *Id.*

[59] Murray & Wunsch, *supra* note 14, at 81.

[60] ROCKEFELLER COMMISSION REPORT, *supra* note 47, at 139. On March 15, 1974, the CIA terminated the CHAOS program. *Id.* The Agency instructed all field offices to turn over any domestic information received (as a byproduct of foreign investigations) to the FBI. *Id.* at 148. The Rockefeller Commission Report made four recommendations regarding the program. *Id.* at 150. First, "Presidents should refrain from directing the CIA to perform what are essentially internal security tasks." *Id.* Second, "[t]he CIA should resist any efforts, whatever their origin, to involve it again in such improper activities." *Id.* Third, "[t]he Agency should guard against allowing any component (like the Special Operations Group) to become so self-contained and isolated from top leadership that regular supervision and review are lost." *Id.* Finally, "[t]he files of the CHAOS project which have no foreign intelligence value should be destroyed by the Agency at the conclusion of the current congressional investigations, or as soon thereafter as permitted by law." *Id.*

[61] *See* S. REP. NO. 94-755, at 3 (1976) [hereinafter CHURCH COMMITTEE REPORT], *available at* http://www.aarclibrary.org/publib/church/reports/book3/contents.htm (last visited Nov. 15, 2004). Two years after the FBI started its COINTELPRO operations, J. Edgar Hoover wrote a book on overcoming the communist threat. *See* J. EDGAR HOOVER, MASTERS OF DECEIT: THE STORY OF COMMUNISM IN AMERICA AND HOW TO FIGHT IT (1958). Excerpts are available at http://www.icdc.com/~paulwolf/cointelpro/mastersofdeceit.htm (last visited Nov. 15, 2004).

[62] *See* Murray & Wunsch, *supra* note 14, at 78. As mentioned in Part II.B *supra*, Hoover started amassing these records at the direction of Attorney General A. Mitchell Palmer.

[63] CHURCH COMMITTEE REPORT, *supra* note 61, at 3.

employer to get a target fired . . . to using the IRS to audit a professor, not just to collect any taxes owed, but to distract him from his political activities."[64]

According to the Church Committee – a Senate Select Committee formed to investigate the activities of the FBI during the mid 1970s – the Agency conducted 2,700 such COINTELPRO operations.[65] "The unexpressed major premise of the programs was that a law enforcement agency has the duty to do whatever is necessary to combat perceived threats to the existing social and political order."[66] The FBI somehow kept these programs secret for fifteen years.[67] However, the Agency finally terminated all COINTELPRO operations in 1971 due to a "threat of public exposure."[68]

---

[64] *Id.* at 8. One of Hoover's most famous targets was Dr. Martin Luther King:

> The FBI's effort to discredit Dr. King and to undermine the SCLC involved plans touching on virtually every aspect of Dr. King's life. The FBI scrutinized Dr. King's tax returns, monitored his financial affairs, and even tried to establish that he had a secret foreign bank account. Religious leaders and institutions were contacted in an effort to undermine their support of him, and unfavorable information was "leaked" to the press. Bureau officials contacted members of Congress, and special "off the record" testimony was prepared for the Director's use before the House Appropriations Committee. Efforts were made to turn White House and Justice Department Officials against Dr. King by barraging them with unfavorable reports and, according to one witness, even offering to play for a White House official tape recordings that the Bureau considered embarrassing to King.

Id. at 131.

[65] *Id.* at 8. When the Church Committee was conducting its investigation, the FBI produced several documents which supported an FBI contention that various Attorneys General, Presidential advisors, members of the House Appropriations Subcommittee, and members of the Presidential Cabinet were, at the very least, put on notice of several COINTELPRO operations. *Id.* at 11.

[66] *Id.* at 3. The tactics included surveillance and infiltration, dissemination of false information, creation of group conflict, repeatedly arresting activists to interfere with their group participation, and participation in assaults and assassinations. *See* Natsu Taylor Saito, *Whose Liberty? Whose Security? The USA PATRIOT Act in the Context of COINTELPRO and the Unlawful Repression of Political Dissent*, 81 OR. L. REV. 1051, 1081-88 (2002). For example, the FBI would place agents within certain groups to advocate violence and illegal activity that, if carried out, could be used to take the group down. *Id.* at 1085.

[67] CHURCH COMMITTEE REPORT, *supra* note 61, at 3.

[68] *Id.* On March 8, 1971, someone broke into the FBI office in Media, Pennsylvania, stealing several documents that included references to the COINTELPRO programs. *Id.* At the time, the "COINTELPRO" phrase was unknown outside the Bureau. Whoever took the documents released them to the press, which prompted reporter Carl Stern to file a Freedom of Information Act lawsuit to obtain additional information on COINTELPRO activities. *Id.* Soon thereafter, the FBI decided to terminate all COINTELPRO operations. *Id.* at 3

D. *The Red Squads of the 1960s and 70s*

While the FBI and CIA monitored the activities of activists, political leaders, and ordinary citizens across the country, several state and local police organizations conducted rigorous surveillance programs on a local level.[69] In New York, for example, the Bureau of Special Services collected intelligence files with more than one million documents on dissident individuals and groups, including records on the Mayor of New York City.[70] In Chicago, undercover agents from the city's police department infiltrated community action organizations and the department's intelligence unit created dossiers on scores of the city's civic leaders, politicians, and journalists.[71] When the extent of these and other organizations' surveillance practices became apparent in the mid-seventies, churches, political groups, civil liberties organizations, and individual activists in New York, Chicago, and Memphis initiated a series of federal civil rights lawsuits in an attempt to curtail their cities' intelligence programs.[72]

Initially, the police departments in New York and Chicago filed motions to dismiss, which the courts denied.[73] The Memphis Police

---

n.1.

[69] *See* Paul G. Chevigny, *Politics and Law in the Control of Local Surveillance*, 69 CORNELL L. REV. 735 (1984).

[70] *See* David Burnham, *City Has Its Own Special Police to Keep Dossiers on Dissidents*, N.Y. TIMES, Aug. 8, 1969, at A30; *See also* Chevigny, *supra* note 69, at 749. In *Handschu v. Special Services Division,* 349 F. Supp. 766 (S.D. N.Y. 1972) ("*Handschu I*") the complaint filed against the New York Police Department also alleged that the Department used agents to infiltrate political and social organizations. According to the plaintiffs, the police collected membership lists of lawful organizations and established reports on individuals based on their membership in these groups. *Id.* at 769-70.

[71] Seth S. King, *Police in Chicago Kept Dossiers on Civic Leaders and Newsmen*, N.Y. TIMES, Mar. 23, 1975, at A34. Chicago's undercover agents became active members in groups like "the Metropolitan Area Housing Alliance, . . . the Rev. Jesse Jackson's People United to Save Humanity . . . and the Alliance to End Police Repression, which concerned itself with cases of alleged police brutality." *Id.* One undercover agent became so involved in the group he was monitoring that he was elected president. *Id.*

[72] Chevigny, *supra* note 69, at 747.

[73] *See* ACLU v. City of Chicago, 431 F. Supp. 25 (N.D. Ill. 1976); Alliance to End Repression v. Rochford, 407 F. Supp. 115 (N.D. Ill. 1975); *Handschu I*, 349 F. Supp. 766, 767-68 (S.D. N.Y. 1972) (refusing to grant defendant's motion to dismiss). The two actions in Chicago eventually consolidated into one. In the New York trial, *Handschu*, the defendants submitted, in support of their motion to dismiss, an affidavit from the New York City Police Commissioner defending the practices of the Bureau of Special Services. *Handschu,* 349 F. Supp. at 767. The Commissioner stated that "the practices and procedures followed by [the Bureau of Special Services] in carrying out its intelligence functions [were] within the scope of the duties imposed by the New York City Charter to protect the

Department, on the other hand, responded by hastily destroying all of its intelligence files.[74] The Memphis plaintiffs obtained a temporary restraining order to prevent further file destruction, but Memphis's Mayor and Chief of Police claimed that they had destroyed the files before the order was served.[75] This claim turned out to be false, as some of the "destroyed" files later appeared in police department offices outside the intelligence section.[76]

As a result of the suits in Chicago, New York, and Memphis, the City of Los Angeles also started destroying its collection of more than two million intelligence files.[77] As was the case in Memphis, however, some of the "destroyed" files later reappeared.[78] One detective with the Los Angeles police force even stored some of the files at his home.[79] When this and other information related to the scandal came to light, the Los Angeles City Council passed an ordinance giving the subjects of the police department's investigations limited access to the intelligence files.[80] Yet, the City Council failed to place controls on future surveillance practices until "forced to do so by the pressure of litigation."[81] On the eve of trial, the Council approved a settlement that gave the plaintiffs $900,000 and placed new restrictions on police investigations.[82]

---

health, safety, and welfare of the public." *Id.*

74 *See* Chevigny, *supra* note 69, at 751-52.

75 *Id.* at 752.

76 *Id.* This appears to be a common theme among police departments that decide to destroy intelligence files. *See Files Not for the Taking*, DENVER POST, Jan. 10, 2003, at B6.

77 Chevigny, *supra* note 69, at 768-69. The City also adopted a new set of regulations, which provided that the intelligence division of the police department could only investigate groups or individuals that disrupt, or assist in disrupting, the public order. *Id.* at 769. In later months, further revelations showed that the intelligence division had been keeping "files on major and minor politicians, a judge, and the President of the Board of Police Commissioners, its own oversight body." *Id.* at 770-71.

78 *Id.* at 771-72.

79 *See id.* at 772. A similar event took place in Oregon. Despite Oregon law, a former Portland terrorism expert carried thirty-six boxes of "spy files" to his barn, where they stayed until 1987. *Files Not for the Taking*, *supra* note 76. Later, the files ended up with a *Portland Tribune* columnist. *Id.*

80 Chevigny, *supra* note 69, at 773.

81 *Id.*

82 *Id.* Los Angeles's consent decree requires the LAPD to have a "reasonable and articulated suspicion" that a group or individual is planning, threatening, or attempting to commit a "significant disruption of the public order" before it can initiate an investigation. *Id.* (citing the Los Angeles Consent Decree). The decree defines "significant disruption of the public order" as "unlawful acts which can reasonably be expected to result in death,

Eventually, Memphis, Chicago, and New York also signed consent decrees that placed strict limitations on their police departments' surveillance practices.[83] Generally, the cities agreed to implement internal annual audits of their police departments, place limitations on dissemination of material obtained through investigation, and establish internal bureaucratic review of questionable cases.[84] Chicago even agreed to an external audit once every five years.[85]

However, both New York and Chicago recently convinced their respective court systems to modify the cities' consent decrees to grant their police departments greater investigatory freedom.[86] For instance, the Seventh Circuit agreed that Chicago had a right to restoration of control over its activities, reasoning that "[t]he era in which the Red Squad flourished is history, along with the Red Squad itself. The instabilities of that era have largely disappeared . . . [and] [t]he culture that created and nourished the Red Squad has evaporated."[87]

Unfortunately, the Seventh Circuit's reasoning is flawed.[88] Consider, for example, the City of Denver, Colorado. Denver recently admitted that it too had a Red Squad during the 1960s and 1970s.[89]

---

serious bodily injury or significant property damage and which are intended to have such results to further societal objectives, to influence societal action or to harass on the basis of race, religion or national origin." *Id.* at 773 n.236 (citing the Los Angeles Consent Decree).

[83] *See id.* at 747-67.

[84] *Id.* at 752-57.

[85] *Id.* at 756-57. For a detailed discussion of the settlement process and the settlement itself, see *Alliance to End Repression v. City of Chicago*, 561 F. Supp. 537 (N.D. Ill. 1982) (approving the Chicago Consent Decree).

[86] *See* Alliance to End Repression v. City of Chicago, 237 F.3d 799 (7th Cir. 2001); Handschu v. Special Services Division, 273 F. Supp. 2d 327 (S.D.N.Y. 2003).

[87] *Alliance to End Repression*, 237 F.3d at 802. Additionally, the court stated:

> If police get wind that a group of people have begun meeting and discussing the desirability of committing acts of violence in pursuit of an ideological agenda, a due regard for the public safety counsels allowing the police department to monitor the statements of the group's members, to build a file, perhaps to plant an undercover agent.

Id. This is the exact type of rationale that police department's used in the 1950s-70s to monitor, infiltrate, and harass organizations that the police believed to be communist sympathizers. *Id.*

[88] *See* Robert Dreyfuss, *The Cops are Watching You*, THE NATION, June 3, 2002, *available at* http://www.thenation.com/docprint.mhtml?i=20020603&s=dreyfuss. (last visited Mar. 9, 2004) ("From New York to Chicago, from Florida to California, police departments are creating, rebuilding or strengthening intelligence units and antiterrorism squads."). The instabilities of the 1950s-70s that were caused by the communist threat have reappeared in the twenty-first century because of the ever-present terrorist threat. *See id.*

[89] Judith Graham, *Denver's Secret Files on Citizens Arouse Outrage: Police Began*

Denver also admitted that it never destroyed the files it collected during those periods despite originally claiming that they had.[90] In fact, the city's police department not only retained its collection of files on Colorado citizens, it continued to build that collection over the next thirty years.[91] The department's files grew to cover 3,200 individuals and 208 organizations.[92] "Many of those people did nothing more than attend peaceful protests at the state Capitol or go to meetings of groups that police decided might represent a threat to public order."[93] Thus, the instabilities of the Red Squad era have not disappeared and the culture that nourished the Red Squads remains intact. In fact, as the following section explains, federal and state governments continue to rely on these instabilities to justify their recent expansion and maintenance of surveillance programs that purport to fight terror.[94]

III. History Repeats Itself: Surveillance Developments During the "War on Terror"

An understanding of the current war on terror within the context of United States history is necessary to fully appreciate the significance of recent government decisions on the "proper balance between national security and civil rights."[95] The Total Information Awareness program ("TIA") and the Multi-State Antiterrorism Information Exchange ("Matrix") – like the Alien and Sedition Acts, the FBI, the CIA, and the surveillance forces during the Red Scares before – were created in times when the United States government believed in the existence of a

---

Spying in the 50s, CHI. TRIB., Jan. 27, 2003, at 7; *see also Files Not for the Taking*, *supra* note 76.

90 Graham, *supra* note 89; *see also Files Not for the Taking*, *supra* note 76. Initially, the city claimed that it destroyed all such files in 1999 when it transferred its records to computers. *Id.* However, in September 2002, six filing cabinets full of old intelligence files unexplainably appeared. *Id.* The material in those files dated back to at least the 1980s. *Id.* Soon thereafter, Denver officials admitted that the city began spying in the 1950s. *Id.*

91 *See id*; *see also Files Not for the Taking*, *supra* note 76.

92 Graham, *supra* note 89.

93 *Id.* In discussing the recent growth of antiterrorist and intelligence units across the country, Robert Dreyfuss noted that, "[i]ronically, all this is occurring in the complete absence of any actual terrorist activity." Dreyfuss, *supra* note 88. Some of the momentum for the growth in surveillance units is simply coming from police departments "taking the opportunity to expand their powers." *Id.*

94 *See* Dreyfuss, *supra* note 88 ("From New York to Chicago, from Florida to California, police departments are creating, rebuilding or strengthening intelligence units and antiterrorism squads.").

95 *See* Cohen, *supra* note 27, at 1433.

significant threat to national security. Additionally, the leaders of the TIA and Matrix programs – like the leaders of the various programs before – made significant efforts to reassure the public that they will not use TIA or the Matrix improperly against innocent Americans.[96] However, history shows that such reassurances are unreliable at best.[97] Thus, programs like the TIA and the Matrix need additional scrutiny to protect the public from potential unconstitutional excess.[98]

A. *Total Information Awareness*

As the predecessor to the Matrix, the TIA garnered significant criticism for its potential threat to individual privacy. Developed by DARPA's Information Awareness Office – which was under the direct control of the Pentagon – the TIA was a "sweeping computer surveillance initiative" designed to collect massive amounts of personal data on American citizens.[99] According to DARPA, however, the agency did not design the program as a tool for spying on innocent Americans: "The TIA research and development program aims to integrate information technologies into a prototype to provide tools to better detect, classify, and identify potential *foreign* terrorists."[100]

Nevertheless, even if the government did not intend to frighten the Orwell-reading public, it succeeded in doing so. The TIA surveillance program collected billions of records on *all American citizens,* regardless of whether the government actually suspected them of being

---

[96] *See, e.g.*, STATE OF GEORGIA, OFFICE OF HOMELAND SECURITY, MATRIX AND ATIX: INFORMATION PROGRAMS DEVELOPED IN RESPONSE TO SEPTEMBER 11, 2001, at 1 (Aug. 1, 2003).

[97] *See supra* Part II.

[98] *See* Skinner v. Ry. Labor Executives Ass'n, 489 U.S. 602, 635 (1989) (Marshall, J. dissenting) ("Precisely because the need for action against [terrorism] is manifest, the need for vigilance against unconstitutional excess is great.").

[99] Hulse, *supra* note 4; *see also* Safire, *supra* note 5.

[100] DARPA REPORT, *supra* note 4, at 3. The DARPA report stated that the goal of the TIA program was "to increase the probability that authorized agencies of the United States can preempt adverse actions." *Id.* To accomplish this task, the TIA would have used a controversial technique called data mining. *Id.* "The core notion behind data mining is that an automated process like a computer algorithm can sift through trillions of pieces of information about millions of people and accurately direct the attention of screeners towards the relative handful who harbor terrorist or other criminal intentions." AMERICAN CIVIL LIBERTIES UNION, DATA MINING MOVES INTO THE STATES at 4 (2004) [hereinafter DATA MINING MOVES INTO THE STATES], *available at* http://www.aclu.org/Privacy/Privacy.cfm?ID=14254&c=130 (last visited Nov. 15, 2004).

potential terrorists.[101]

> Every purchase you make with a credit card, every magazine subscription you buy and medical prescription you fill, every Web site you visit and e-mail you send or receive, every academic grade you receive, every bank deposit you make, every trip you book and every event you attend – all these transactions and communications will go into what the Defense Department describes as "a virtual, centralized grand database."[102]

The Pentagon planned to use this information – along with criminal history records, address histories, driver's license information, etc. – as part of a large-scale data mining project that would attempt to predict future terrorist events based on the past habits or actions of American individuals.[103] Yet, no evidence existed that the program would even work.[104] Information in such large-scale databases is often wrong and the error rate could be disgracefully high, which would result in wrongful accusations against innocent citizens.[105] Additionally, the potential for government abuse of such a system is extraordinarily high, and the simple fact that the government has access to such vast amounts of personal data is somewhat Orwellian in nature.[106]

---

[101] Safire, *supra* note 5.

[102] *Id.* The Office of Information Awareness, as part of the new antiterrorist surveillance system, also worked on a radar-based device that identifies people by the way they walk. *See* Maureen Dowd, *Walk This Way: Slouching Towards Orwell*, ORLANDO SENTINEL, May 22, 2003, at A19.

[103] *See Government Data Mining: Hearing Before the Subcomm. on Technology, Information Policy, and Intergovernmental Relations*, 108th Cong. 1-5 (2003) (statement of Paula B. Dockery, Chairman, Florida Senate Committee on Home Defense, Public Security and Ports) *available at* http://reform.house.gov/uploadedfiles/dockery.pdf (last visited Nov. 15, 2004). The system employed decision trees, deviation detection, algorithms, and image analysis. *Id.* at 1.

[104] *See Government Data Mining: Hearing Before the Subcomm. on Technology, Information Policy, Intergovernmental Relations and the Census of the House Comm. on Government Reform*, 108th Cong. (2003) (statement of Barry Steinhardt, Director, American Civil Liberties Union), *available at* http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12669&c=206 (last visited Nov. 15, 2004).

[105] *See id.*; BUREAU OF JUSTICE STATISTICS, USE AND MANAGEMENT OF CRIMINAL HISTORY RECORD INFORMATION: A COMPREHENSIVE REPORT, 2001 UPDATE 38 (Dec. 2001) (admitting that "inadequacies in the accuracy and completeness of criminal history records is the single most serious deficiency affecting the Nation's criminal history record information."); *Shared Databases Bore Through Privacy Barriers*, MILWAUKEE J. SENT., Dec. 30, 2003, at 6E (describing how a sales manager at Hilton Hotels was fired because Hilton relied on erroneous information in a commercial database that said the employee had a criminal history).

[106] *See, e.g.*, Jeffrey Rosen, *How to Protect America, and Your Rights*, N.Y. TIMES, Feb.

Even the logo for the Information Awareness Office – "Scientia Est Potentia," which translates to "Knowledge Is Power" – inspired comparisons between the TIA and Orwell's *1984*.[107] Scripted below an all-seeing eye that was perched atop an Egyptian pyramid, the slogan sounded eerily similar to Big Brother's party slogan: "War is Peace, Freedom is Slavery, Ignorance is Strength."[108] Chosen by the head of the Information Awareness Office, Admiral John Poindexter – who was convicted after the Iran-Contra affair on five felony counts of lying in Congressional testimony, destroying official documents, and obstructing a congressional inquiry – the program's slogan confirmed Poindexter's complete lack of political awareness.[109]

In an attempt to dispel some of the fears over the TIA program, and to salvage his position as head of the Information Awareness office, Poindexter eliminated the panoptic eye and pyramid from TIA's logo and changed the program's name from *Total* Information Awareness to *Terrorist* Information Awareness.[110] However, this slight change in style did nothing to quell the public's suspicions over the program's substance. In fact, some of these suspicions were confirmed when Congress learned that Poindexter created a TIA website where investors could bet on the likelihood of future terrorist attacks.[111]

Dubbed the Policy Analysis Market, the site would have rewarded traders that correctly forecasted terrorist attacks, assassinations, and political coups.[112] "Traders bullish on a biological attack on Israel or

---

6, 2004, at A27 ("In its current form, the system poses a significant danger that unscrupulous state officials will conduct dragnets in search of crimes that have nothing to do with terrorism.") For a recent example of how government employees mishandled and improperly disclosed personal information, *see* DEP'T OF HOMELAND SEC., PRIVACY OFFICE, REPORT TO THE PUBLIC ON EVENTS SURROUNDING JETBLUE DATA TRANSFER (Feb. 20, 2004) (discussing the Transportation and Safety Administration's improper role in obtaining passenger data from jetBlue Airlines and ensuring that jetBlue transferred the information to a private corporation).

107 *See Total Information Awareness*, *supra* note 8.

108 ORWELL, *supra* note 1, at 4.

109 *Total Information Awareness*, *supra* note 8. An appeals court overturned Poindexter's conviction because Congress granted Poindexter immunity for his testimony. *See* Safire, *supra* note 5.

110 *See* Ariana Eunjung Cha, *Pentagon Details New Surveillance System: Critics Fear Proposed Extensive Use of Computer Database Raises Privacy Issues*, WASH. POST, May 21, 2003, at A06. For a comparison of the old and new logos of the Information Awareness Office, see the ACLU's Total Information Awareness page at http://www.aclu.org/Privacy/Privacy.cfm?ID=14729&c=130 (last visited Feb. 21, 2004).

111 *See* Hulse, *supra* note 4.

112 *Id.*

bearish on the chances of a North Korean missile strike" would have had the opportunity to wager on the likelihood of such an event.[113] In defense of the program, the Defense Department blandly stated: "Research indicates that markets are extremely efficient, effective and timely aggregators of dispersed and even hidden information."[114] What the Defense Department did not mention, however, was the potential for market manipulation by the terrorists that would be carrying out the events.[115] Since all traders would have traded with complete anonymity, terrorists could have participated in the trading and profited from their terrorist activities.[116]

The congressional furor surrounding the Policy Analysis Market added momentum to an effort to completely eliminate funding for the Office of Information Awareness.[117] The uproar also convinced Poindexter to resign from government service.[118] However, it did not prevent other government agencies from attempting to create programs that are substantially similar to the TIA.[119]

B. *Multi-State Antiterrorism Information Exchange*

In 2003, Florida announced that it was partnering with a private corporation, SeisInt, Inc., to develop the Matrix.[120] According to the

---

113 *Id.*

114 *Id.*

115 *Id.*

116 *See* Hulse, *supra* note 4. The Web site for the Policy Analysis Market still exists at http://www.policyanalysismarket.org. However, no information is currently available through the site as of Nov. 15, 2004. After Congress learned about the program, the White House, which had allocated eight million dollars to fund the site through 2005, ordered the Office of Information Awareness to alter the site so that market events that were visible earlier in the day could no longer be seen. *Id.*

117 *Id.* Senator Ron Wyden sponsored a bill in February of 2003 that temporarily cut-off funds for the TIA program. *Id.* The bill stated that no agency of the government could appropriate funds to the program for 90 days, during which time the Department of Defense had to issue a detailed report on the TIA program. *See* H.R. Res. 2, 108th Cong. (2003); *see also* Cha, *supra* note 110. The Defense Department issued the report, but Congress eliminated funding for the program anyway after learning about the Policy Analysis Market. *See* DARPA REPORT, *supra* note 4, at 3; Hulse, *supra* note 4.

118 Eric Schmitt, *Poindexter Will Be Quitting Over Terrorism Betting Plan*, N.Y. TIMES, Aug. 1, 2003, at A11.

119 *See* O'Harrow, *supra* note 1.

120 *Id.* In Florida's 2003 Annual Report on Domestic Security, the state's Domestic Security Oversight Board stated that one of the foundations of Florida's security strategy was to "Improve Information Intelligence and Technology." FLORIDA'S DOMESTIC SECURITY OVERSIGHT BOARD, 2003 ANNUAL REPORT, USING STATE AND FEDERAL FUNDS TO

Georgia Office of Homeland Security, "Matrix is an informational program developed to increase and enhance the exchange of sensitive terrorism and other criminal activity information between local, state, and federal enforcement agencies."[121] However, even though developers of the Matrix ostensibly set up the program to allow law enforcement officials to fight crime and terrorism, data on law-abiding citizens constitutes the majority of the information in the database.[122] In fact, the program is "designed to . . . analyze billions of records about both criminals and *ordinary Americans*."[123]

The records in the Matrix program come from a mix of government and commercial databases.[124] However, Matrix officials have not released a complete list of the information actually contained within the system. Nevertheless, Matrix officials have admitted that they use the following data, which is available from public databases:

- Credit information
- Driver's license photographs
- Marriage and divorce records
- Past addresses and telephone numbers
- Names and addresses of family members
- Neighbors' addresses and telephone numbers
- Business associates
- The make, model and color of registered vehicles
- Speeding tickets
- Arrests
- Social security numbers and dates of birth[125]
- Bankruptcies
- Liens and judgments
- UCC filings
- Concealed weapons permits
- FAA aircraft and pilots licenses
- Hunting and fishing licenses

MAKE FLORIDA SAFER 1 (Sept. 2003).

121 STATE OF GEORGIA, *supra* note 96, at 1 (Aug. 1, 2003).

122 Gast, *supra* note 9, at F1 (citing statement of Gerald M. Haskins, Professor of Computer and Information Science and Engineering, University of Florida).

123 O'Harrow, *supra* note 1 (emphasis added).

124 DATA MINING MOVES INTO THE STATES, *supra* note 100, at 1.

125 *Id.* at 1-2.

- Professional licenses
- Voter registration records[126]

This is a fairly comprehensive list of personal information that is publicly available on private individuals. Yet, it does not include all of the information that may be available through the Matrix's admitted use of commercial databases. "Given the information available in today's commercial databases . . . the range of detail accessible through the program could well be even greater, extending into such areas as purchasing habits, magazine subscriptions, demographic information, and lifestyle categorizations."[127] The records available in commercial databases may even include student loan status, prescription lists, abortion records, and political and religious affiliations.[128]

Oscar Gandy described the technology that collects and processes this information as the "panoptic sort."[129] Essentially, the panoptic sort collects information on the everyday lives of individuals and then categorizes those individuals based on their social, political, and consumer preferences.[130] The Matrix employs a technique called "data mining" that is based on this same categorization principle.[131] "The core notion behind data mining is that an automated process like a computer algorithm can sift through trillions of pieces of information about millions of people and accurately direct the attention of screeners towards the relative handful who harbor terrorist or other criminal

---

126 Brief of Amici Curiae Electronic Privacy Information Center (EPIC) et al. at 12-13, Hiibel v. Sixth Judicial District Court of Nevada, Humboldt County, 124 S. Ct. 430 (2003) (No. 03-5554) [hereinafter Brief of Amici Curiae Electronic Privacy Information Center].

127 DATA MINING MOVES INTO THE STATES, *supra* note 100, at 2.

128 SYKES, *supra* note 2, at 29. Acxiom, owner of one of the world's largest commercial databases of consumer information, holds detailed records on nearly every United States citizen. *See* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1473-74 (2000); *see also* Acxiom, Core Competencies, Database, http://www.acxiom.com/default.aspx?ID=1768&Country_Code=USA (last visited Nov. 15, 2004) ("Acxiom creates and manages some of the largest databases in the world."). The government is increasingly collecting information from private entities to develop databases of personal information. Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1095 (2002). For example, ChoicePoint has contracts with approximately thirty-five federal agencies, including the FBI and IRS. *Id.* The company's database holds over ten billion records, which were gathered from sources that include private detectives and credit reporting agencies. *Id.*

129 OSCAR H. GANDY, JR., THE PANOPTIC SORT, A POLITICAL ECONOMY OF PERSONAL INFORMATION 15 (1993).

130 *See id.*, at 15. The three functions of the panoptic sort, according to Gandy, are: identification, classification, and assessment. *Id.*

131 *See* DATA MINING MOVES INTO THE STATES, *supra* note 100, at 4.

intentions."[132]

Defenders of the Matrix deny that it is a data mining program and assert that the system simply "includes information that has always been available to investigators but brings it together and enables police to access it with extraordinary speed."[133] This is incorrect on at least three counts. First, law enforcement officers have never had routine access to the commercial data available in the Matrix.[134] Second, in the Institute for Intergovernmental Research's application for a four million dollar Justice Department grant to fund the Matrix system, the Institute listed that one of the objectives of the Matrix was to "develop and pilot test a model *data mining* and integration system for terrorist and other intelligence information."[135] Finally, creating a program that combines isolated, independently available databases of information on innocent American citizens is not simply a "technological advancement;" it is a significant setback to the basic American principle that the government will let people alone unless it has cause to suspect them of wrongdoing.[136]

Even those closely associated with the Matrix freely admit to the potential intrusiveness of the data mining system. "It's scary. It could be abused. I mean, I can call up everything about you, your pictures and pictures of your neighbors," stated Phil Ramer, special agent in charge of Florida's statewide intelligence.[137] Data mining is a powerful tool. Indeed, the fact that the TIA employed data mining was one of the reasons that Congress eliminated funding for the TIA program.[138] Now,

---

132 *Id.*

133 O'Harrow, *supra* note 8.

134 AMERICAN CIVIL LIBERTIES UNION, *Matrix: Myths and Reality* 2 (Feb. 10, 2004) [hereinafter MYTHS AND REALITY], *available at* http://www.aclu.org/Privacy/Privacy.cfm?ID=14894&c=130 (last visited March 5, 2004).

135 *Id.* (citing INSTITUTE FOR INTERGOVERNMENTAL RESEARCH, AN APPLICATION TO PROVIDE INFORMATION TECHNOLOGY AND INTELLIGENCE SHARING SUPPORT TO THE MULTISTATE PILOT PROJECT TO EXCHANGE TERRORISM AND OTHER INTELLIGENCE INFORMATION). Additionally, "documents obtained by the ACLU [through several Freedom of Information Act requests] contain numerous explicit references to data mining, including meeting minutes of the Matrix board, presentations by the Florida Department of Law Enforcement, and in FDLE budget documents." *Id.*

136 DATA MINING MOVES INTO THE STATES, *supra* note 100, at 3.

137 O'Harrow, *supra* note 1.

138 *See* Hulse, *supra* note 4. Congress has proactively passed a few other privacy protecting measures as well. For example, the Communications Privacy Act of 1984 prohibits cable operators from monitoring subscribers' viewing habits. *See* 47 U.S.C. § 551 (2002). Also, the Video Privacy Protection Act prohibits the release of video rental

however, the executive branch of the federal government is attempting to avoid Congress's elimination of federal data mining programs by establishing the same systems through state cooperation.[139] In 2003, the Justice Department and the Department of Homeland Security pledged $12 million to the State of Florida to set up the Matrix system.[140] Thus, thwarted by Congress in its attempt to create the TIA, the Bush Administration now encourages states to pick up where the TIA left off.[141]

Thirteen states originally pledged to participate in this endeavor.[142] Yet, eight of those states have since dropped out.[143] However, while only Florida, Ohio, Pennsylvania, Michigan, and Connecticut remain, these states represent a considerable percentage of the United States population.[144] Moreover, several other states are still considering membership in the Matrix program.[145] Thus, the Matrix continues to

---

data. *See* Communications Privacy Act of 1984, 47 U.S.C. § 551 (2000); Video Privacy Protection Act, 18 U.S.C. § 2710 (2000).

139 *See* DATA MINING MOVES INTO THE STATES, *supra* note 100, at 4; O'Harrow, *supra* note 1.

140 O'Harrow, *supra* note 1.

141 *See id.*

142 DATA MINING MOVES INTO THE STATES, *supra* note 100, at 4. California and Texas showed an interest but backed out before signing the June 2003 agreement. *Id.*

143 Mark Johnson, *2 More States Pull Out of Anti-Crime Database, New York and Wisconsin Withdrew from the Controversial Matrix Program*, ORLANDO SENTINEL, Mar. 12, 2004, at A12; Mark Johnson, *2 More States Turn Against Massive Anticrime Database*, L.A. TIMES, Mar. 12, 2004, at A30. The states that have either dropped out or declined to participate include: Alabama, California, Colorado, Georgia, Louisiana, Kentucky, New York, Oregon, South Carolina, Texas, Utah, West Virginia, and Wisconsin. *Id.*

144 Johnson, *supra* note 143. Ohio and Connecticut, however, are also having second thoughts. In Connecticut, for example, lawmakers in the state recently scheduled hearings to determine whether the program's usefulness outweighs privacy concerns. *See* Lisa Chedekel, *Legislators Wary of Matrix System*, HARTFORD COURANT, Feb. 4, 2004, at B9. In Ohio, the Governor has decided to review the State's involvement. *See* Jon Craig, *State Sold Ohioan's Driving Records to Florida Database*, COLUMBUS DISPATCH, March 14, 2004, at 4C. Ohio first sold the driver records to the Matrix in October, 2002. *Id.* However, state officials did not release this information until nearly two years later when questioned about their participation in the program. *See* Bill Bush, *Ohio May Join in Multistate Database: Some Say Anti-Terrorism Program Too Intrusive, Backers Tout its Reach*, COLUMBUS DISPATCH, Oct. 25, 2003, at A01 ("Ohio is *considering* providing Matrix with driver and motor-vehicle registrations. . . .") (emphasis added).

145 *See* Jon Chesto, *Pol Wants State Cops to Join Info Database*, BOSTON HERALD, Feb. 24, 2004, at O32 (discussing Massachusetts's potential membership in the Matrix); *Decision on 'Matrix' Database Postponed*, COMMERCIAL APPEAL, Feb. 4, 2004, at B6 (discussing Tennessee's possible membership in the Matrix system); *Entering the Matrix: Iowans Deserve Full Public Debate on New Database*, OMAHA WORLD-HERALD, Feb. 11, 2004, at

present a significant threat to individual privacy and the need to scrutinize the program remains.

IV. Restoring Privacy after the Matrix

> That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society.[146]

The existing legal framework surrounding informational privacy is failing, as programs like the Matrix render old laws obsolete.[147] In an effort to address this problem, the remainder of this Article discusses two ways to challenge the repressive potential of the Matrix system: (1) seeking an injunction against the operation of the Matrix program under the First and Fourteenth Amendments of the United States Constitution,[148] and (2) lobbying for state legislative action in the form of consent decrees that either (a) place strict limitations on the program's operations, or (b) eliminate funding for the program entirely.[149] None of these options are perfect and, for various reasons, none may work. The most likely option for short-term success, however, comes from the legislative approach.[150]

B8 (discussing Iowa's possible membership in the Matrix).

146 Warren & Brandeis, *supra* note 11, at 193.

147 *See* DeVries, *supra* note 27, at 306 ("The changes wrought by digital technology . . . are so deep and broad that the old laws and theories are not adapting fast enough. New, privacy invasive technological practices may solidify into new social norms, and future generations will not know to challenge them.").

148 In addition to the problems discussed later in this section, Eleventh Amendment sovereign immunity places some limitations on the effectiveness of litigation against the Matrix. Since SeisInt is Florida's partner in developing the Matrix, and receives its funding from the State, it might be considered an "arm of the state" and receive Eleventh Amendment sovereign immunity protections. For a detailed discussion of the Eleventh Amendment and its effects on litigation against states or state officials, see Scott Dodson, *The Metes and Bounds of State Sovereign Immunity*, 29 HASTINGS CONST. L.Q. 721 (2002); Alfred Hill, *In Defense of Our Law of Sovereign Immunity*, 42 B.C. L. REV. 485 (2001). In short, the best way to avoid Eleventh Amendment obstacles is to sue, in his or her individual capacity, the state and Matrix officials that are in charge of the operating the Matrix system. *See Ex parte* Young, 209 U.S. 123, 169 (1908). For a discussion on how the Fourth Amendment protections are implicated by the collection and compilation of personal information, see Solove, *supra* note 128.

149 *See infra* Part IV.C.

150 *See id.*

A. *Protecting the First Amendment Right to Free Association*

1. Surveillance under *Laird v. Tatum*

The First Amendment preserves the government's right to collect publicly available information.[151] However, the First Amendment also protects each citizen's right to belong to lawful social or political associations.[152] Consequently, the government cannot collect publicly available information in a manner that objectively "chills" a citizen's right to free association.[153] Yet, what constitutes an objective chill is open for debate.[154]

In *Laird v. Tatum*, the Supreme Court refused, in a 5–4 decision, to enjoin the United States Army from establishing a database containing records on civilian political activists.[155] In 1967, President Johnson ordered Army troops to Detroit, Michigan, to assist local authorities in deterring potential civil unrest.[156] Once there, soldiers attended public meetings, researched general publications, and obtained information from civilian law enforcement agencies in an effort to monitor political dissidents.[157] Army officials then forwarded all information collected

---

151 *See* Froomkin, *supra* note 128, at 1508 ("The First Amendment protects the freedom of speech and of the press, but does not explicitly mention the right to gather information. However, both the Supreme Court and appellate courts have interpreted the First Amendment to encompass a right to gather information.").

152 *See* NAACP v. Alabama, 357 U.S. 449, 462 (1958); *see also* Elrod v. Burns, 427 U.S. 347, 356-60 (1976).

153 *See* Laird v. Tatum, 408 U.S. 1, 11-15 (1972); *see also* Socialist Workers Party v. Attorney General, 419 U.S. 1314 (1974) (surveillance that deters supporters from joining an organization, even if surveillance is in public, does present a case or controversy under Article III).

154 *Compare* Philadelphia Yearly Meeting of Religious Soc'y of Friends v. Tate, 519 F.2d 1335, 1337-38 (3d Cir. 1975) (following *Laird* and stating that police surveillance of public meetings, by itself, was "legally unobjectionable"), *with* Presbyterian Church v. United States, 870 F.2d 518 (9th Cir. 1989) (holding that active surveillance of church services, which resulted in decreased attendance, created an objective harm for purposes of Article III's case or controversy requirement).

155 *Laird*, 408 U.S. at 1. A total of four justices dissented in two separate opinions. Arguing for the right to be free from overbearing surveillance, Justice Douglas stated:

> When an intelligence officer looks over every nonconformist's shoulder in the library, or walks invisibly by his side in a picket line, or infiltrates his club, the America once extolled as the voice of liberty heard around the world no longer is cast in the image which Jefferson and Madison designed . . . .

Id. at 28-29 (Douglas, J., dissenting).

156 *Id.* at 4-5.

157 *Id.* at 6.

through this surveillance to Army Intelligence Headquarters in Fort Holabird, Maryland, where officials stored the information in a central database.[158]

According to the plaintiffs in *Laird*, the compilation and storage of this information effectively prohibited them from freely exercising their First Amendment rights.[159] However, the Supreme Court found that the Army had a right to collect these records, as the simple "existence and operation of the intelligence gathering and distributing system" did not establish a "specific present objective harm or a threat of specific future harm."[160] According to the Court, the plaintiffs' claims were less significant than other activities that it had previously condemned on First Amendment grounds, so the Court classified the plaintiffs' injuries as purely subjective.[161] Thus, the plaintiffs' claim did not meet the case

---

[158] *Id.* at 13-14. When Congress learned about the scope of the Army's surveillance practices, it convened hearings to express its concerns. *Id.* at 7. Afterwards, the Army ordered a significant reduction in the scope of its program. "For example. . . the records in the computer data bank at Fort Holabird were found unnecessary and were destroyed, along with other related records." *Laird*, 408 U.S. at 13-14.

[159] *Id.*

[160] *Id.* at 3, 14. According to the majority, "[a]llegations of a subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm." *Id.* at 13-14. In reaching this decision, the majority stated that "it is significant that the principal sources of information were the news media and publications in general circulation." *Id.* at 6. The dissent, of course, disagreed with the majority's position that no objective harm exsisted, stating that "the present controversy is not a remote, imaginary conflict." *Id.* at 26 (Douglas, J. dissenting). The plaintiff's fear was that "permanent reports of their activities will be maintained in the Army's databank, and their 'profiles' will appear in the so-called 'Blacklist' and that all of this information will be released to numerous federal and state agencies upon request." *Id.* at 25 (Douglas, J. dissenting). "One need not wait to sue until he loses his job or until his reputation is defamed." *Laird*, 408 U.S. at 26 (Douglas, J. dissenting).

[161] *See id.* at 11-14. The *Laird* Court cited a number of cases protecting freedom of association: Baird v. State Bar of Arizona, 401 U.S. 1 (1971) (holding that a state may not require persons to disclose their associations in order to receive admission to the state bar); *see also* Keyishian v. Bd. of Regents, 385 U.S. 589 (1967) (holding that a state cannot fire employees merely because of their political associations); Lamont v. Postmaster General, 381 U.S. 301 (1965) (holding that a state cannot require persons to send individual written requests to the Post Office in order to receive mailings of certain types of political literature); Baggett v. Bullitt, 377 U.S. 360 (1964) (holding that a state could not require persons to take an oath of vague and uncertain meaning as a condition of employment). According to the Court in *Laird*, these decisions recognize that "governmental action may be subject to constitutional challenge even though it has only an indirect effect on the exercise of First Amendment rights." *Laird*, 408 U.S. at 12-13. However, the Court also stated that these decisions in no way eroded the "established principle that to entitle a private individual to invoke the judicial power to determine the validity of executive or legislative action he must show that he has sustained or is immediately in danger of

or controversy requirement of Article III.[162]

2. Establishing Article III Standing

Since *Laird*, lower courts have struggled to determine when a surveillance system creates an objective harm for purposes of Article III standing.[163] As *Laird* suggested, when the surveillance only involves police attendance at meetings that are open to the public, a court is unlikely to find that objective harm is involved.[164] On the other hand, when police surveillance has specific adverse effects on an individual, or group of individuals, the First Amendment claim is justiciable,[165] even if the surveillance is purely in the public realm.[166] Thus, to establish

---

sustaining, a direct injury as the result of that action . . . ." *Id.* at 13 (quoting *Ex Parte* Levitt, 302 U.S. 633, 634 (1937)).

[162] *See id.* at 14 ("[T]he federal courts established pursuant to Article III of the Constitution do not render advisory opinions.") (quoting United Pub. Workers v. Mitchell, 330 U.S. 75, 89 (1947)).

[163] *See, e.g.*, Alliance to End Repression v. City of Chicago, 627 F. Supp. 1044, 1048 (N.D. Ill. 1985).

[164] *See Laird*, 408 U.S. at 6; *see also* Philadelphia Yearly Meeting of Religious Soc'y of Friends v. Tate, 519 F.2d 1335, 1337-38 (3d Cir. 1975) (following *Laird* and stating that police surveillance of public meetings, by itself, was "legally unobjectionable.").

[165] *See* Alliance to End Repression, 627 F. Supp. at 1048-49 (N.D. Ill. 1985); *see also* Anderson v. Davila, 125 F.3d 148, 160 (3d Cir. 1997) (holding that a government surveillance operation aimed at two individuals that was initiated in response to one of those individuals filing a discrimination suit against the police department constituted a "specific present harm"); Presbyterian Church v. United States, 870 F.2d 518 (9th Cir. 1989) (holding that active surveillance of church services, which resulted in decreased attendance, created an objective harm for purposes of Article III case or controversy requirement); Ozonoff v. Berzak, 744 F.2d 224 (1st Cir. 1984) (holding that government "loyalty check" that was required of applicants to the World Health Organization prevented free exercise of First Amendment rights); Clark v. Lib. of Cong., 750 F.2d 89 (D.C. Cir. 1984) (holding that a library worker who was investigated by the FBI because of political associations met case or controversy requirement of Article III when he alleged that the investigation harmed his reputation and cost him employment opportunities); Paton v. La Prade, 524 F.2d 862 (3d Cir. 1975) (holding that FBI plan – in conjunction with the United States Post Office – to track written communications with the Socialist Workers Party in New York City constituted a specific harm since the files created as a result of this plan caused injury to future educational and employment opportunities).

[166] *See* Socialist Workers Party v. Attorney Gen., 419 U.S. 1314 (1974) (surveillance that deters supporters from joining an organization, even if surveillance is in public, does present a case or controversy under Article III). *Id.* Even if the surveillance program only monitors public activities or information, the plaintiff can still meet Article III's case or controversy requirement in order to argue the case on its merits. *Id.* In *Socialist Workers Party*, the plaintiffs alleged that the FBI planned to attend and monitor the SWP's upcoming convention. *Id.* Justice Marshall found that the plaintiffs' allegations were specific enough, under *Laird*, to meet Article III's case or controversy requirement. *Id.* However, Justice

Article III standing, plaintiffs must show some specific adverse effect.[167] According to *Laird*, plaintiffs can make this showing by proving either: (1) that a surveillance system creates a "specific present objective harm," or (2) that the surveillance creates a "threat of specific future harm."[168]

For the first ten years following *Laird*, establishing a present objective harm was fairly straightforward. For example, alleging that an investigation disrupted a political association by deterring supporters from joining the group would present a justiciable claim.[169] Alternatively, showing that the dissemination of false or misleading investigative reports harmed the plaintiff's reputation would suffice to satisfy Article III standing requirements.[170] However, after the United States Supreme Court's 1983 decision in *City of Los Angeles v. Lyons*,[171] showing only a present or past objective harm is not enough to establish justiciability.[172] Plaintiffs must additionally allege that the government's violation of First Amendment rights will repeat itself in the future.[173]

Marshall went on to state that the plaintiffs did not have a compelling case on the merits. *Id.* at 1319; *see also* Berlin Democratic Club v. Rumsfeld, 410 F. Supp. 144 (D. D.C. 1976). The court in *Berlin Democratic Club* summarized the requirements for finding a justiciable claim by stating:

> [W]hile collection and retention of information, if collected in a legal manner, cannot be challenged, public dissemination of that information in a false or defamatory manner and with no lawful purpose, disruption of legitimate activities, termination of employment, illegal electronic surveillance, and other forms of harassment are subject to challenge as beyond 'legitimate surveillance activities.'

Id. at 151.

167 *See supra* note 165.

168 *See supra* note 160.

169 *See Presbyterian Church*, 870 F.2d at 521-22 (holding that active surveillance of church services, which resulted in decreased attendance, created an objective harm for purposes of Article III case or controversy requirement); Founding Church of Scientology v. FBI, 459 F. Supp. 748, 760 (D.D.C. 1978) (holding that surveillance of church activities presented a justiciable claim because it deterred others from joining the church).

170 *See Berlin Democratic Club*, 410 F. Supp. at 151 (finding a justiciable claim where plaintiffs made sufficient allegations that an Army surveillance project went beyond simple collection and retention of information to disseminating that information with a defamatory purpose); Jabara v. Kelley, 476 F. Supp. 561 (E.D. Mich. 1979) (holding that allegations of the FBI's dissemination of false and misleading reports to other federal agencies presented a justiciable claim), *vacated in part on other grounds by* Jabara v. Webster, 691 F.2d 272 (6th Cir. 1982).

171 461 U.S. 95 (1983).

172 *See id.*

173 *See id.* In *Lyons*, the plaintiff was seeking an injunction against the Los Angeles

Yet, *Lyons* should not affect standing under the "threat of specific future harm" test for showing an objective harm because, if proven, a threat of specific future harm, by definition, has the potential to take place at some point in the future, thereby satisfying the *Lyons* standing requirement.

In *Socialist Workers Party v. Attorney General*, the Supreme Court had to decide whether the FBI's plan to attend and monitor a meeting of the Young Socialist Alliance ("YSA") would constitute a threat of future specific harm under *Laird v. Tatum*.[174] After rejecting the government's contention that surveillance must be regulatory, proscriptive, or compulsory before the Court could grant standing, Justice Marshall found that the plaintiffs' allegations were sufficiently specific to establish a case or controversy under Article III.[175] "[T]he applicants have complained that the challenged investigative activity will have the concrete effects of dissuading some YSA delegates from participating actively in the convention and leading to possible loss of employment for those who are identified as being in attendance."[176]

Subsequent lower court cases adopted "potential injury to future employment" as a factor in determining justiciability.[177] In *Paton v. La Prade*, for example, the Third Circuit held that the FBI's retention of files on all persons who wrote letters to the Socialist Workers Party ("SWP") had the potential to interfere with future employment or

---

Police Department ("LAPD") to prevent its officers from using chokeholds, except in situations where the person being apprehended threatened the use of deadly force. *Id.* The plaintiff alleged that he was stopped by LAPD officers for a routine traffic violation and, even though he offered no resistance, the officers seized him and applied a chokehold, which rendered him unconscious and damaged his larynx. *Id.* at 97. The Supreme Court held that Lyons did not have standing to bring suit for injunctive relief because "[p]ast exposure to illegal conduct does not in itself show a present case or controversy regarding injunctive relief . . . if unaccompanied by any continuing, present adverse effects." *Id.* at 95 (citing O'Shea v. Littleton, 414 U.S. 488, 495-96 (1974)).

174 *See Socialist Workers Party*, 419 U.S. at 1317-18.

175 *Id.* at 1318. The government was relying on a passage from *Laird* which discussed previous cases where the Court found that state actions violated the First Amendment. "[I]n each of these cases, the challenged exercise of governmental power was regulatory, proscriptive, or compulsory in nature, and the complainant was either presently or prospectively subject to the regulations, proscriptions, or compulsions that he was challenging." *Id.* (quoting *Laird*, 408 U.S. at 11). Justice Marshall stated that the government read *Laird* too broadly. "In the passage relied upon by the Government, the Court was merely distinguishing earlier cases, not setting out a rule for determining whether an action is justiciable or not." *Socialist Workers Party*, 419 U.S. at 1318.

176 *Id.* at 1319.

177 *See, e.g.*, Paton v. La Prade, 524 F.2d 862 (3d Cir. 1975).

educational opportunities, thus establishing a "threat of specific future harm" and meeting *Laird*'s standing requirements.[178] *La Prade* involved FBI surveillance of Lori Paton, a high school student enrolled in a social studies class that "examined the contemporary political spectrum."[179] As part of an assignment for the class, Paton wrote a letter to the Socialist Workers Party requesting information about the organization.[180] When the letter arrived at the post office in New York, the mail delivery foreman recorded Ms. Paton's name and address from the exterior of the letter and then forwarded the recorded information to the FBI's New York branch.[181]

After receiving Paton's information, the FBI agent assigned to the investigation contacted the chief of police where Paton lived to ask whether Ms. Paton had ever been arrested.[182] Unsatisfied that the answer was no, the FBI agent then proceeded to interview Ms. Paton's principal and vice-principal, who informed the agent about the nature of Paton's homework assignment.[183] Finally content that Ms. Paton was not involved in subversive activities, the agent recommended that the FBI administratively close the case.[184] However, the FBI created a permanent record of the investigation and placed Paton's name in the local FBI file index, which it labeled with the symbol "SM-SWP" (Subversive Matter-Socialist Workers Party).[185]

Paton claimed that the FBI's retention of such a file threatened her future educational and employment opportunities and the Third Circuit agreed, holding that "the threatened injury gives Paton standing to challenge retention of the file."[186] Accordingly, the allegation that a

---

178 524 F.2d 862, 868 (3d Cir. 1975).

179 *Id.* at 865.

180 *Id.*

181 *Id.*

182 *Id.* If an investigation of an individual has the effect of deterring others from associating with that individual, that weighs in favor of justiciability. *See* Jabara, 476 F. Supp. 561, 568 (E.D. Mich. 1979).

183 *Paton*, 524 F.2d at 866.

184 *Id.*

185 *Id.* Disseminating information collected in a false or misleading manner is also a factor in favor of justiciability. *See Jabara*, 476 F. Supp. at 568.

186 *Paton*, 524 F.2d at 868. The Third Circuit did not rule on the merits of Paton's case. It did, however, list several factors to consider in determining whether a surveillance program creates an objective chill:

> Factors to be weighed in balancing are the accuracy and adverse nature of the information, the availability and scope of dissemination of the records, the legality of the methods by which the information was compiled, the

surveillance system threatened future educational or employment opportunities qualified as a "threat of specific future harm" for purposes of establishing justiciability.[187]

Thus, in summary, *Laird v. Tatum* held that plaintiffs challenging a surveillance system have to show either a current or past objective harm, or a threat of specific future harm in order to have standing to sue. Allegations of a subjective chill are not sufficient to make a claim justiciable.[188] Additionally, after *City of Los Angeles v. Lyons*, simply showing a present or past objective harm by itself is not enough to establish justiciability.[189] Plaintiffs must now allege that the government's violation of First Amendment rights will repeat itself in the future.[190] Finally, *Socialist Workers Party* and cases like *Paton v. La Prade* clarified *Laird* by holding that injury to future educational or employment opportunities should qualify as a "threat of specific future harm."[191]

3. Does the Matrix Create an Objective Chill?

In holding that the Army's surveillance database did not create an objective harm, *Laird* stated that "it is significant that the principal sources of information were the news media and publications in general circulation."[192] In this regard, Matrix officials claim that the system only collects information that is publicly available.[193] If true, *Laird* could possibly bar any First Amendment claim against Florida's use of the system.[194] However, there are two reasons why any "public information" argument should not preclude Article III standing in a claim against the Matrix program.

> existence of statutes authorizing the compilation and maintenance, and prohibiting the destruction, of the records, and the value of the records to the Government.

Id. at 869.

187 *See id.*

188 *See* Laird v. Tatum, 408 U.S. 1, 11 (1972).

189 *See* 461 U.S. 95 (1983).

190 *See id.*

191 *See* Socialist Workers Party v. Attorney Gen., 419 U.S. 1314 (1974) (surveillance that threatens employment opportunities does present a case or controversy under Article III); *Paton*, 524 F.2d at 865-68 (surveillance that potentially injures future educational or employment opportunities presents a justiciable claim).

192 *Laird*, 408 U.S. at 6.

193 *See* O'Harrow, *supra* note 1; Gast, *supra* note 9.

194 *See Laird*, 408 U.S. at 6.

First, the type of information collected by the Matrix is entirely different from what the Army collected in *Laird*. In *Laird*, the Army's main sources of information were readily available news publications.[195] The Matrix, on the other hand, relies on information that is far more personal and not so easily obtainable. It contains social security numbers, dates of birth, driver's license photographs, voter registration records, and untold information from the Matrix's admitted use of commercial databases.[196] Law enforcement officials have never had routine access to the commercial data available in the Matrix.[197]

Second, even if a court decides that the information collected by the Matrix is publicly available under *Laird*, that is only one factor the court must use in determining whether a claim against the Matrix is justiciable. The court would still have to decide whether the State's use of the information it collects prevents an individual or group of individuals from exercising their First Amendment rights.[198]

Unfortunately, no one knows exactly what Matrix officials do with the information they collect.[199] Thus, it is difficult to determine whether the state participants use information stored in the Matrix in a manner that objectively harms anyone's exercise of First Amendment rights. Accordingly, the *Laird / City of Los Angeles v. Lyons* standing requirement poses a serious obstacle to challenging the State's use of the Matrix program on First Amendment grounds. While the collection of such personal information intuitively seems objectionable, the collection by itself is not enough to establish a First Amendment violation.[200] One must show a specific objective harm committed by the State, that the State will repeat in the future, or a "specific threat of

---

195 *Id.*

196 *See* DATA MINING MOVES INTO THE STATES, *supra* note 100, at 1-2; Brief of Amici Curiae Electronic Privacy Information Center, *supra* note 126, at 12-13. "Given the information available in today's commercial databases . . . the range of detail accessible through the program could well be even greater, extending into such areas as purchasing habits, magazine subscriptions, demographic information, and lifestyle categorizations." DATA MINING MOVES INTO THE STATES, *supra* note 100, at 2.

197 MYTHS AND REALITY, *supra* note 134, at 2.

198 *See* Socialist Workers Party v. Attorney Gen., 419 U.S. 1314 (1974) (surveillance that deters supporters from joining an organization, even if surveillance is in public, does present a case or controversy under Article III).

199 For example, if a law student buys a subscription to *Harper's* or *Mother Jones*, does someone from the Florida Department of Law Enforcement contact the Dean of the law school to ask if the student has subversive tendencies? For a similar situation, *see Paton*, 524 F.2d at 868.

200 *See Laird*, 408 U.S. at 1.

future harm" in order to establish a justiciable claim.[201] Without knowing how the State uses information in the Matrix system, it is difficult, if not impossible, to meet these requirements.

B. *Selective Disclosure: Exploring the Fourteenth Amendment's General Right to Privacy*

While the First Amendment embodies a specific form of privacy interest, the right to privacy in one's associations, the Fourteenth Amendment contains the Constitution's general right to privacy.[202] Largely developed by the Warren and Burger Courts during the 1960s and 1970s, this Fourteenth Amendment protection focuses on an individual's "right to be let alone."[203]

Generally, the Supreme Court has characterized this right as dealing with "matters relating to marriage, procreation, contraception, family relationships, and child-rearing and education."[204] However, at least two cases suggest a rather significant exception to this general rule.[205] In *Whalen v. Roe*[206] and *Nixon v. Administrator of General*

---

[201] *See* City of Los Angeles v. Lyons, 461 U.S. 95 (1983); *Laird*, 408 U.S. at 13-14 (1972).

[202] *See* Roe v. Wade, 410 U.S. 113, 153 (1973); Whalen v. Roe, 429 U.S. 589, 600 n.23 (1977). For a detailed explanation of the development of the right of privacy under the United States Constitution, see Gerald B. Cope, Jr., Note, *Toward a Right of Privacy as a Matter of State Constitutional Law*, 5. FLA. ST. U. L. REV. 631, 659-81 (1977). To establish a liberty interest under the Fourteenth Amendment, plaintiffs must pass the three-part balancing test developed by the Supreme Court in *Matthews v. Eldridge*, 424 U.S. 319 (1976).

> First, the private interest that will be affected by the official action; second, the risk of an erroneous deprivation of such interest through the procedures used, and the probable value, if any, of additional or substitute procedural safeguards; and finally, the Government's interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirement would entail.

Id. at 335. Essentially, this would require plaintiffs challenging the Matrix to weigh their privacy interests against: (1) the risk that the Matrix will erroneously invade that privacy, and (2) the government's efficiency interest in maintaining the Matrix database. *Id.*

[203] *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). *See* SYKES, *supra* note 2, at 91-92; Cope, *supra* note 202, at 646-47. While the Court did not fully develop its privacy doctrine until the middle of the Twentieth Century, the phrase "right to be let alone" originated from Thomas Cooley's work in the late 1800s, and was popularized by Justices Warren and Brandeis in their article. *Id.*

[204] *See* Paul v. Davis, 424 U.S. 693, 713 (1976); Whalen v. Roe, 429 U.S. 589, 600 n.26 (1977).

[205] Cope, *supra* note 202, at 670.

Services,[207] the Court strongly implied that the Constitution protects the right to informational privacy.[208] While neither of these cases actually upheld the privacy right asserted, both recognized the need to protect individuals from the disclosure of personal information.[209]

1. *Databanks and Information Privacy under* Whalen v. Roe

Whalen involved a constitutional challenge to a New York statute that regulated the use of prescription drugs.[210] In 1972, based on a concern "that drugs were being diverted into unlawful channels," the New York Legislature passed a statute that required the State to record dangerous drug prescriptions in a state-run database.[211] Under the statute, doctors could only prescribe certain potentially harmful drugs by filling out an official form and filing that form with the State Health Department.[212] Officials at the Health Department then recorded the information on tapes for storage in a local database, where each record remained for five years before being destroyed.[213]

A few days before the New York statute became effective, a group of patients and doctors challenged the legislation as a violation of the Fourteenth Amendment's general right to privacy.[214] According to the plaintiffs, a genuine risk existed that the information in the database would become public and that publicity of this information would adversely affect the patients' reputations.[215] Consequently, this concern caused some patients to refrain from taking, and prompted some doctors

---

206 429 U.S. 589 (1977).

207 433 U.S. 425 (1977).

208 Richard C. Turkington, *Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy*, 10 N. ILL. UNIV. L. REV. 479, 497 (1990).

209 *Id.* at 498; Cope, *supra* note 202, at 680.

210 *See* Whalen v. Roe, 429 U.S. 589 (1977).

211 *Id.* at 589. The statute classified drugs in five schedules. *Id.* Illegal drugs that have no prescribed medical value and are subject to abuse – such as heroin – were classified as Schedule I. *Id.* Schedules II through V include drugs that have a progressively lower chance for abuse but also have a recognized medical value. *Id.* The drugs at issue in *Whalen* were Schedule II, the most dangerous of the legitimate drugs. *Id.*

212 *Id.* at 593. The form included the name of the prescribing physician, the name of the dispensing facility, the name and dosage of the drug, and the patient's name, address, and age. *Id.*

213 *Id.*

214 *Id.* at 595-600. The group included patients that used Schedule II drugs, the doctors that prescribed them, and two associations of physicians. *Id.*

215 *Whalen*, 429 U.S. at 595-600.

to stop prescribing, certain types of medication.[216] These factors, according to the plaintiffs, impaired their "interest in the nondisclosure of private information and also their interest in making important decisions independently."[217]

In response, the Supreme Court formally recognized the possibility of a right to privacy for one's personal information: "The cases sometimes characterized as protecting 'privacy' have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions."[218] However, the Court held that the New York statute, on its face, did not "pose a sufficiently grievous threat to either interest to establish a constitutional violation."[219] In support of its decision, the Court noted that New York ran its database "offline," so that no one outside the computer room could access the information, and that a Department of Health statute expressly prohibited public disclosure of the patients' identities.[220] Since the plaintiffs failed to show any instances where the State of New York mishandled information in the database, the Court

---

216 *Id.* at 600. The plaintiffs presented parental testimony about their children's fear of being stigmatized. *Id.* at 595 n.16. At least one child had already stopped taking medication because of this concern. *Id.* Three adult patients testified as to their fear of intentional or unintentional disclosure and the harm that would result. *Id.* One of those patients even decided to obtain his drugs from another state. *Id.* Even though the court recognized evidence that certain people were negatively affected by the New York regulation, it refused to invalidate the statute because "about 100,000 prescriptions for such drugs were being filled each month prior to the entry of the District Court's injunction. Clearly, therefore, the statute did not deprive the public of access to the drugs." *Id.* at 603.

217 *Id.* at 600.

218 *Id.* at 598-600. In support of the first privacy interest, the right to avoid disclosure of personal matters, the Court cited: Justice Brandeis's dissent in *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (characterizing "the right to be let alone" as "the right most valued by civilized men"); Griswold v. Connecticut, 381 U.S. 479, 483 (1965) (recognizing that privacy is protected by the "penumbras" and "emanations" of the Bill of Rights); Stanley v. Georgia, 394 U.S. 557 (1969); California Bankers Ass'n v. Schultz, 416 U.S. 21, 79 (1974) (Douglas, J., dissenting); California Bankers Ass'n v. Schultz, 416 U.S. 21, 79 (1974) (Powell, J., concurring).

219 *Whalen*, 429 U.S. at 600.

220 *Id.* at 594-95. In the twenty months after the statute took effect, state officials only used the information twice in investigations involving alleged drug abuse by patients. *Id.* at 595. Based on this information, the District Court held that the regulation was unnecessary. *Id.* at 596. After pointing out that such *Lochner*-era reasoning was improper, the Supreme Court disagreed, stating that "[s]tate legislation which has some effect on individual liberty or privacy may not be held unconstitutional simply because a court finds it unnecessary, in whole or in part. *Id.* at 597.

had no proof that these safeguards were insufficient to protect their privacy interests.[221] Thus, the Court refused to enjoin the state's use of the reporting program.[222]

2. Nixon v. Administrator of General Services *and the Right to Personal Information Privacy*

Nixon v. Administrator of General Services involved President Nixon's challenge to the Presidential Recordings and Materials Preservation Act (Act).[223] While President Nixon challenged the Act on several grounds, none of which involved the Fourteenth Amendment, the significant feature of *Nixon* is that the Court, citing *Whalen v. Roe,* again recognized "the individual interest in avoiding disclosure of

---

[221] *Id.* at 601-02. "There is no support in the record, or in the experience of the two States that New York has emulated, for an assumption that the security provisions of the statute will be administered improperly." *Id.* at 601. In a footnote, the Court discussed *Buckley v. Valeo*, 424 U.S. 1 (1976), where the Court refused to invalidate the reporting requirements of the Federal Election Campaign Act of 1971 on the asserted ground that the Act's disclosure requirements would prevent persons from contributing money to minority parties. *Id.* at 601 n.27. According to the Court, "clearly articulated fears" are not enough to enjoin a reporting requirement where the state has a legitimate interest in gathering the information. *Id.* This is similar to the rational in *Laird v. Tatum, supra* Part IV(A)(1)(a)-(c). According to *Laird*, "[a]llegations of a subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm." *Laird*, 408 U.S. at 13-14.

Interestingly, the Court in *Whalen* recognized that certain people would refuse to take medication because of the New York regulation. "Unquestionably, some individuals' concern for their own privacy may lead them to avoid or to postpone needed medical attention." *Whalen*, 429 U.S. at 602. However, it refused to invalidate the statute because "about 100,000 prescriptions for such drugs were being filled each month prior to the entry of the District Court's injunction. Clearly, therefore, the statute did not deprive the public of access to the drugs." *Id.* at 603.

[222] *Whalen*, 429 U.S. at 603-04. "We hold that neither the immediate nor the threatened impact of the patient-identification requirements in the New York State Controlled Substances Act of 1972 . . . is sufficient to constitute an invasion of any right or liberty protected by the Fourteenth Amendment." *Id.* Since the Court was faced with a system with adequate privacy safeguards, it did not "decide any question which might be presented by the unwarranted disclosure of accumulated private data – whether intentional or unintentional – or by a system that did not contain comparable security provisions." *Id.* at 605-06. Several lower courts have addressed the appropriateness of finding information privacy as a constitutional right. *See* Barry v. City of New York, 712 F.2d 1554, 1559 (2d Cir. 1983) ("Most courts considering the question . . . appear to agree that privacy of personal matters is a protected interest.").

[223] *See* 433 U.S. 425 (1977). While *Nixon*'s privacy challenge was under the First, Fourth, and Fifth Amendments, and not the Fourteenth Amendment, the Court's decision in *Nixon* is significant in relation to this Article because it reaffirmed *Whalen*'s suggestion that the constitution does protect information privacy. *See generally id.*

personal matters."[224] The Court held that Nixon did have a reasonable expectation of privacy in his presidential materials, but decided that it would have to weigh this reasonable expectation against the public interest in viewing Nixon's materials and the privacy safeguards included in the Act.[225] "[Nixon's] claim of invasion of his privacy cannot be considered in the abstract; rather, the claim must be considered in light of the specific provisions of the Act, and any intrusion must be weighed against the public interest in subjecting the Presidential materials of [Nixon's] administration to archival screening."[226]

Under this balancing test, the Court observed that Nixon's claim was weaker than the claim presented in *Whalen v. Roe*.[227] Only a small portion of the "42 million pages of documents and 880 tape recordings" in question actually qualified as private materials.[228] According to the Court, "[n]ot only does the Act challenged here mandate regulations similarly aimed at preventing undue dissemination of private materials but, unlike *Whalen*, the Government will not even retain long-term control over such private information; rather, purely private papers and recordings will be returned to [Nixon] under . . . the Act."[229] Thus, the Court held that the Act contained sufficient privacy safeguards and that the public interest in viewing the presidential materials outweighed any small risk of improper disclosure.[230]

---

224 *Id.* at 457 (citing *Whalen*, 429 U.S. at 599).

225 *Nixon*, 433 U.S. at 457-58.

226 *Id.* at 458.

227 *Id.*

228 *Id.* at 456. "[T]he Act 'is a reasonable response to the difficult problem caused by the mingling of personal and private documents and conversations in the midst of a vastly greater number of nonprivate documents and materials related to government objectives.'" *Id.*

229 *Id.* at 458-59.

230 *Id.* at 465. The Court did state that Nixon had a reasonable expectation of privacy in his presidential materials. *Id.* at 457. However, it performed a balancing test to determine whether that interest was outweighed by countervailing concerns. *Id.* at 456. The other factors the Court considered included: the limited intrusion of the screening process, the fact that an overwhelming majority of the materials were not private in nature, the public interest in preserving the presidential materials, and the "impossibility of segregating the small amount of private materials without comprehensive screening." *Id.* Furthermore, according to the Court, the Act was sensitive to the President's privacy interests and the archivists had an unblemished record of discretion. *Id.*

3. The Fourteenth Amendment and the Matrix

While the Court decided neither *Whalen* nor *Nixon* on behalf of the plaintiffs, both cases suggested that, under the right circumstances, the government's acquisition and recordation of information may violate privacy rights under the Constitution.[231] The *Whalen* Court even specifically announced a concern for the government's use of computer databases: "[w]e are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."[232] Accordingly, there is a chance that the Court would invalidate a program like the Matrix if it found that the program failed to meet Fourteenth Amendment privacy standards.[233]

After *Whalen* and *Nixon*, the key to making this showing is convincing the Court that the program's privacy safeguards are insufficient.[234] In *Whalen*, for example, the plaintiffs failed on this ground.[235] Holding in favor of the State, the Court relied on the fact that New York ran its database "offline," and only a limited number of state officials had access to the system.[236] Significantly, the plaintiffs did not show specific instances where the State violated security provisions of the program.[237]

Plaintiffs challenging the Matrix, however, should have an easier time showing deficiencies in the program's privacy safeguards than their counterparts did in *Whalen*. The Matrix system is not "offline," and numerous law enforcement officers in the participating states can access the database.[238] Additionally, a private company operates the Matrix, and Hank Asher, the company's founder, has a significant criminal record.[239] "In 1999, the Drug Enforcement Administration and the FBI suspended information service contracts with an earlier Asher-

231 Turkington, *supra* note 208, at 498.

232 *Whalen*, 429 U.S. at 605.

233 *See id.*

234 *See id.*; Nixon v. Adm'r of Gen. Serv., 433 U.S. 425, 457-58 (1977).

235 *Whalen*, 429 U.S. at 594-95.

236 *Id.*

237 *Id.* at 601. "There is no support in the record, or in the experience of the two States that New York has emulated, for an assumption that the security provisions of the statute will be administered improperly." *Id.*

238 *See* DATA MINING MOVES INTO THE STATES, *supra* note 100; Gast, *supra* note 9, at F1.

239 *See* O'Harrow, *supra* note 1; Craig, *supra* note 144.

run company because of concerns about his past."[240]

This combination of factors makes the privacy safeguards of the Matrix far less protective than those found in *Whalen*. However, because of the program's age and Matrix officials' unwillingness to release information about the systems operation, plaintiffs challenging the Matrix probably will not be able to show specific instances where Matrix officials mishandled personal information. Consequently, the reviewing court probably will not assume that Matrix officials or the participating states will use the information improperly.[241]

The court may also employ a balancing test, similar to the one in *Nixon*, and weigh the potential privacy risk against the public interest in "national security."[242] Considering the current conservative nature of the Supreme Court,[243] if the case ever proceeds that far, "national security" will almost certainly outweigh threats to individual privacy, especially if plaintiffs cannot produce specific examples of how Matrix, or state officials, improperly used information contained in the database.[244] Thus, a reviewing court, similar to the Court in *Whalen*, might allow Florida to act as a testing ground for the experimental law enforcement program.[245]

---

240 O'Harrow, *supra* note 1. Asher is a former drug smuggler and was once accused of participating in a plot to assassinate former Nicaraguan President Daniel Ortega. *See id.*; Craig, *supra* note 144.

241 *Whalen*, 429 U.S. at 601. This was a significant factor in the *Whalen* Court's decision in favor of the state. *Id.*

242 *See Nixon*, 433 U.S. at 465. "National security" is a common justification for passing legislation or establishing programs that diminish civil liberties such as privacy. *See supra* Part II. For example, Matrix officials justify their program on its potential to combat terrorism. *See* STATE OF GEORGIA, *supra* note 96, at 1. However, "[e]ven though Matrix is ostensibly set up to allow law enforcement officials to fight terrorism and crime, data about perfectly law-abiding citizens makes up the predominant portion of that database." Gast, *supra* note 9 (statement of Gerald M. Haskins, Professor of Computer and Information Science and Engineering, University of Florida). The real justification for the Matrix system is that it will enhance police departments' power to conduct everyday law enforcement activities, not to fight terrorism. *See* Dreyfuss, *supra* note 88.

243 *See* DAVID G. SAVAGE, TURNING RIGHT: THE MAKING OF THE REHNQUIST SUPREME COURT (1992). In an article Chief Justice Rehnquist authored in the mid-1970s, he expressed concerns about expanding the right of privacy at the expense of effective law enforcement. William Rehnquist, *Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement? Or: Privacy, You've Come a Long Way, Baby*, 23 KAN. L. REV. 1 (1974).

244 *See* City of Los Angeles v. Lyons, 461 U.S. 95 (1983). If plaintiffs challenging the Matrix cannot show a harm that is likely to be repeated in the future, they may lose on standing grounds because of *Lyons*. *See id.*

245 *See Whalen*, 429 U.S. at 597. On this point, the *Whalen* Court cited Justice

C. *Encouraging Legislative Action*

Since so little is known about the Matrix itself and how Matrix or state officials use information contained within the system, courts currently may be unable to invalidate the program on privacy grounds.[246] However, legislatures in participating states are not so restricted and may ban news gathering technology if they: (1) do so through a law of general application, and (2) reasonably tailor the ban to achieve some legitimate governmental objective.[247] Privacy is certainly such an objective.[248] Therefore, considering the judiciary's current inability to address the privacy threat of the Matrix, state legislatures have a responsibility to act. As the Court of Appeals for the District of Columbia stated in *Menard v. Mitchell*:

> A heavy burden is placed on all branches of Government to maintain a proper equilibrium between the acquisition of information and the necessity to safeguard privacy. Systematic recordation and dissemination of information about individual citizens is a form of surveillance and control which may easily inhibit freedom to speak, to work and to move about in this land.[249]

There are two ways state legislatures can act to circumscribe the Matrix's operations. First, similar to how Congress shut down the TIA, state legislatures can pass moratoriums on funding for the Matrix program, effectively forcing their respective states to drop out of the system.[250] Starting in 2004, federal funding for the program will end and

---

Brandeis's dissent in *New State Ice Company*, which stated:

> To stay experimentation in things social and economic is a grave responsibility. Denial of the right to experiment may be fraught with serious consequences to the Nation. It is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.

Id. at 597 n.20 (citing New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting)).

246 *See supra* Part IV.B.

247 *See* Froomkin, *supra* note 128, at 1510.

248 *See id.*

249 Menard v. Mitchell, 328 F. Supp. 718, 726 (D.C. Cir. 1971). *Menard* involved a request to remove the plaintiff's fingerprints from criminal records maintained by the FBI. *Id.* at 720. The plaintiff was detained and arrested, but never prosecuted. *Id.* at 723. Thus, the plaintiff requested that his fingerprints be removed from the criminal system. *Id.* at 720. The court refused. *See id.* at 727-28.

250 *See* Hulse, *supra* note 4. Out of the eighteen states that either signed the original Matrix agreement or considered joining the Matrix system, only five remain. *See* Johnson, *supra* note 143. Of the five remaining, at least two states, Connecticut and Ohio, are

the Matrix will cost each participating state about $1.5 million per year in membership fees alone.[251] Cost is a major concern for every participating state and every state that is considering joining the system.[252] In fact, every state that has dropped out of the Matrix has listed cost as one of the factors in its decision.[253] With each state that chooses to deny funding for membership fees – thereby withdrawing from the program – the Matrix loses a significant portion of the data it once contained and its usefulness to existing and potential member states diminishes.[254]

Alternatively, state legislatures may choose to enact certain privacy measures that restrict the Matrix's operations.[255] Such measures may include limitations on the types of information that a state contributes to the database or limitations on how Matrix users may utilize the information contained within the system.[256] Yet, if a state legislature decides to simply limit the scope of the state's participation in the Matrix, rather than dropping out altogether, it should clearly define the limitations it imposes and place an absolute prohibition on future expansions of the state's use of the Matrix system. Government programs that collect personal information often suffer from "mission creep," which refers to the risk than an initially justifiable government

---

reconsidering their membership. *See* Chedekel, *supra* note 144; Craig, *supra* note 144. In Connecticut, lawmakers in the state recently scheduled hearings to determine whether the program's usefulness outweighs privacy concerns. *See* Chedekel, *supra* note 144. In Ohio, the Governor has decided to review the State's involvement. *See* Craig, *supra* note 144.

251 Chesto, *supra* note 145. The Florida Legislature has already allocated $1.6 million to pay SeisInt for its work. O'Harrow, *supra* note 1.

252 *See* Johnson, *supra* note 143.

253 *See id.*

254 *See id.*

255 *See, e.g.*, Chedekel, *supra* note 144 (quoting State Representative Michael Lawlor: "We're prepared to write some privacy safeguards into the law, or, if necessary, to force the state to withdraw from the program."). *But see* DeVries, *supra* note 27, at 291 ("[L]egislatures are unlikely to impose many new limits on government misuse of personal information in the current atmosphere of heightened national security and fear.").

256 *See, e.g.*, Duane D. Stanford & Joey Ledford, *State Can't Give Driver Records to the Matrix*, ATLANTA J. CONST., Oct. 21, 2003, at A1 ("Georgia's attorney general said Monday it would be illegal for the state to turn over millions of driver records to the Matrix crime-fighting database being developed in Florida."). Another way to limit the privacy threat of the Matrix would be for states to lobby Matrix officials to design the system so that users could not connect personal information in the database with an individual's name "unless the system indicated a significant risk for terrorism or other violent crimes." *See* Rosen, *supra* note 106.

program can evolve into a much larger unjustifiable version of itself.[257]

> Consider the 1996 law requiring employers to make quarterly reports on the name, address, Social Security number and wages of each of their employees to the Department of Health and Human Services. The intent of the legislation was to track deadbeat dads. Yet those reports now also go to the Social Security Administration to verify unemployment reports, to the Treasury to cross-check tax deductions and even to the Department of Education to help it find individuals delinquent on their student loans.[258]

Thus, even if state legislatures initially limit the scope of the Matrix system, the risk is very high that sometime in the future – after the initial uproar over the program settles down – law enforcement officials, other branches of government, or maybe even the legislature itself will lobby for expanding the scope of the program to include other, more controversial, uses.

To protect against this risk, state legislatures that choose to remain in the system should establish an independent privacy oversight board to monitor their state's use of the Matrix.[259] The purpose of the oversight committee would be "to protect those persons with whose affairs the community has no legitimate concern."[260] If states choose to maintain their membership in the Matrix, some form of external oversight is necessary to protect individuals' privacy rights from governmental excess. The privacy oversight board would both monitor its state's participation in the Matrix and serve as a check on future legislative action that may attempt to broaden the scope of the program.

V. Conclusion

United States history reveals that state and federal governments often rely on "national security" as a rationale for expanding their

---

257 Peter P. Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, 77 WASH. U. L.Q. 461, 498 (1999).

258 Melanie Scarborough, *Big Brother Virginia*, WASH. POST, Aug. 31, 2003, at B8. Also consider the expanded use of the Social Security Number. When it was introduced during the New Deal, President Roosevelt reassured the public that it would not become a national identity card. *Id.* Over time, however, the SSN has essentially become just that. *See* Swire, *supra* note 257, at 498.

259 External audits were a common feature in the Red Squad settlements of the 1970s. *See* Chevigny, *supra* note 69, at 752-57.

260 Warren & Brandeis, *supra* note 11, at 214.

governing powers at the expense of constitutional rights.[261] From the Alien and Sedition Acts to the excesses of the FBI and CIA, the United States government has habitually overstepped its constitutional powers when faced with a pending national crisis.

Unfortunately, these governmental failures did not result from informed and rational decisions that upholding civil liberties would create unacceptable security risks.[262] Rather, these poor choices were the product of the intermittent nature of our nation's security crises.[263] As Justice Brennan once stated, "[t]he inexperience of decisionmakers in dealing with wartime security claims makes them reluctant to question the factual bases underlying asserted security threats."[264] Consequently, the decision to increase national security at the expense of civil liberties is frequently flawed, and, according to Justice Brennan, "[a]fter each perceived security crisis ended, the United States has remorsefully realized that the abrogation of civil liberties was unnecessary."[265]

Nevertheless, the United States seems unable to prevent itself from repeating this error during times of perceived crisis.[266] The current "war on terror," for example, has spawned several government surveillance initiatives nominally aimed at fighting terrorism. Yet, these programs have the effect of monitoring the everyday activities of ordinary Americans. The Matrix is no exception. Eventually, stories of government excess regarding the Matrix system will emerge, and courts will have the ability to prevent the program's needless invasion of privacy. Until then, state legislatures are the only governmental bodies capable of imposing limitations on the program's reach and guarding their citizens against the program's constitutional excess.

---

261 Murray & Wunsch, *supra* note 14, at 73.

262 William J. Brennan, Jr., *The Quest to Develop a Jurisprudence of Civil Liberties in Times of Security Crises, Address at the Law School of Hebrew University* 1 (Dec. 22, 1987), *available at* http://www.brennancenter.org/resources/downloads/nationsecurity brennan.pdf (last visited Mar. 29, 2004).

263 *Id.*

264 *Id.* at 2.

265 *Id.* at 1.

266 *Id.* "For as adamant as my country has been about civil liberties during peacetime, it has a long history of failing to preserve civil liberties when it perceived its national security threatened." *Id.* According to Brennan, courts should accept some of the responsibility for failing to establish safeguards or policies that protect civil liberties. *Id.* "The peacetime jurisprudence of civil liberties leaves the nation without a tradition of, or detailed theoretical basis for, sustaining civil liberties against particularized security concerns." *Id.*