

DIGITAL DOSSIERS AND THE DISSIPATION OF FOURTH AMENDMENT PRIVACY

DANIEL J. SOLOVE*

I. INTRODUCTION	1084
II. GOVERNMENT INFORMATION GATHERING AND THE PRIVATE SECTOR.....	1089
A. THIRD PARTY RECORDS AND THE GOVERNMENT	1089
B. GOVERNMENT-PRIVATE SECTOR INFORMATION FLOWS.....	1095
C. THE DANGERS OF GOVERNMENT INFORMATION GATHERING	1101
D. PROTECTING PRIVACY WITH AN ARCHITECTURE OF POWER	1114
III. THE FOURTH AMENDMENT, RECORDS, AND PRIVACY.....	1117
A. THE ARCHITECTURE OF THE FOURTH AMENDMENT	1117
1. The Purposes and Structure of the Fourth Amendment	1117
2. Fourth Amendment Scope: Privacy.....	1121
3. Fourth Amendment Structure: Warrants	1124
B. THE SHIFTING PARADIGMS OF FOURTH AMENDMENT PRIVACY.....	1128
C. THE NEW <i>OLMSTEAD</i>	1133
IV. THE NEW ARCHITECTURE OF POWER: THE EMERGING STATUTORY REGIME AND ITS LIMITS	1138
A. STATUTORY REGIME ARCHITECTURE: SCOPE.....	1138
1. Wiretapping and Bugging	1138
2. Stored Communications	1141
3. Records of Communications Providers	1142
4. Pen Registers, E-mail Headers, and Web Surfing	1144
5. Financial Records	1145
6. Electronic Media Entertainment Records.....	1146
7. Medical Records.....	1147
8. Holes in the Regime	1148

* Assistant Professor, Seton Hall Law School; J.D. Yale, 1997. I would like to thank Rachel Godsil, Ted Janger, Orin Kerr, Raymond Ku, Erik Lillquist, Michael Risinger, Paul Schwartz, Christopher Slobogin, Richard Sobel, Charles Sullivan, Michael Sullivan, Peter Swine and Elliot Turrini.

B. STATUTORY REGIME ARCHITECTURE: STRUCTURE	1149
V. RECONSTRUCTING THE ARCHITECTURE	1151
A. SCOPE: SYSTEM OF RECORDS	1152
B. STRUCTURE: REGULATED SUBPOENAS	1159
C. REGULATING POST-COLLECTION USE OF DATA	1166
VI. CONCLUSION	1167

I. INTRODUCTION

In the Information Age, an increasing amount of personal information is contained in records maintained by Internet Service Providers (ISPs), phone companies, cable companies, merchants, bookstores, websites, hotels, landlords, employers and private sector entities. Many private sector entities are beginning to aggregate the information in these records to create extensive digital dossiers.¹

The data in these digital dossiers increasingly flows from the private sector to the government, particularly for law enforcement use. Law enforcement agencies have long sought personal information about individuals from various third parties to investigate fraud, white-collar crime, drug trafficking, computer crime, child pornography, and other types of criminal activity. In the aftermath of the terrorist attacks of September 11, 2001, the impetus for the government to gather personal information has greatly increased, since such data can be useful to track down terrorists and to profile airline passengers for more thorough searches.² Detailed records of an individual's reading materials, purchases, diseases, and website activity enable the government to assemble a profile of an individual's finances, health, psychology, beliefs, politics, interests, and lifestyle.³ This data can unveil a person's anonymous speech and personal associations.⁴

The increasing amount of personal information flowing to the government poses significant problems with far-reaching social effects. Inadequately constrained government information-gathering can lead to at least three types of harms. First, it can result in the slow creep toward a totalitarian state.⁵ Second, it can chill democratic activities and interfere

1. See *infra* Part II.

2. See *infra* Part II.

3. See *infra* Part II.

4. Government access to such data may implicate one's First Amendment rights to freedom of speech and freedom of association. See *infra* Part II.C.

5. See, e.g., DAVID H. FLAHERTY, *PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES* (1989); PAUL M. SCHWARTZ & JOEL R. REIDENBERG, *DATA PRIVACY LAW* 39 (1996); ("[T]otalitarian regimes

with individual self-determination.⁶ Third, it can lead to the danger of harms arising in bureaucratic settings.⁷ Individuals, especially in times of crisis, are vulnerable to abuse from government misuse of personal information. Once government entities have collected personal information, there are few regulations of how it can be used and how long it can be kept. The bureaucratic nature of modern law enforcement institutions can enable sweeping searches, the misuse of personal data, improper exercises of discretion, unjustified interrogation and arrests, roundups of disfavored individuals, and discriminatory profiling.⁸ These types of harms often do not result from malicious intent or the desire for domination. Justice Brandeis was prescient when he observed that people “are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in the insidious encroachment by men of zeal, well-meaning but without understanding.”⁹

The transfer of personal information from the private sector to the government thus requires some form of regulatory control, a way to balance privacy with effective law enforcement. The first source for protecting privacy against infringement by law enforcement agencies is the Fourth Amendment, which prohibits unreasonable searches and seizures and requires that the government first obtain judicial authorization before conducting a search or seizure. According to the Supreme Court, “[t]he overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State.”¹⁰ The Court, however, has held that there is no reasonable expectation of privacy in records maintained by third parties.¹¹ In the void left by the absence of Fourth Amendment protection, a series of statutes provide some limited

in Eastern Europe relied on information gathering and data storage to weaken the individual capacity for critical reflection and to repress any social movements outside their control.”); Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 560 (1995); Peter P. Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, 77 WASH. U. L.Q. 461, 471 (1999) (articulating problems of “how an authoritarian or totalitarian government might use and abuse information about citizens’ financial transactions”).

6. See generally Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815 (2000); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999).

7. I previously explored the contrast between these two types of power in the context of private sector information collection and use. See Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001).

8. See *infra* Part III.

9. *Olmstead v. United States*, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting).

10. *Schmerber v. California*, 384 U.S. 757, 767 (1966).

11. See, e.g., *Smith v. Maryland*, 442 U.S. 735, 743 (1979); *United States v. Miller*, 425 U.S. 435, 444 (1976). For a more extensive discussion of these cases and others, see *infra* Part III.C.

restraints on government access to third party records.¹² The protections of the statutory regime are far less exacting than those of the Fourth Amendment; information can be obtained through mere subpoenas and court orders, which have relatively few constraints and little meaningful judicial oversight. Further, numerous classes of records are not covered at all. Thus, there is a profoundly inadequate legal response to the emerging problem of government access to aggregations of data, “digital dossiers” that are increasingly becoming digital biographies.

A similar scenario unfolded in 1928, when the Supreme Court held in *Olmstead v. United States*¹³ that wiretapping a person’s home telephone did not run afoul of the Fourth Amendment. The Court rigidly adhered to a conception of privacy that recognized only physical invasions, which did not include wiretapping because there was no physical trespass to the home. Following *Olmstead*, Congress enacted § 605 of the Federal Communications Act of 1934 to regulate wiretapping, but the law was grossly ineffective.¹⁴ *Olmstead* left a void in regulating the central threats to privacy in the twentieth century—wiretapping and electronic surveillance—which dramatically increased without adequate regulatory controls and oversight.¹⁵ In 1967, the Court overruled *Olmstead*.¹⁶ Today, it remains a relic of the past, a long discredited decision. It symbolizes the Court’s lack of responsiveness to new technology, unwarranted formalism in its constitutional interpretation, and failure to see the larger purposes of the Fourth Amendment.

Despite the fact that *Olmstead* was overruled, its spirit has been reincarnated. The new *Olmstead* era, and its full implications are just beginning to emerge. The Court’s current conception of privacy is as a form of total secrecy.¹⁷ As conceived by the Court, an individual’s hidden world should be protected. It has expressed an interest in safeguarding the intimate information that individuals carefully conceal. Privacy is about protecting the skeletons that are meticulously hidden in the closet. Since information maintained by third parties is exposed to others, it is not

12. See *infra* Part IV.

13. 277 U.S. 438, 464 (1928).

14. For a discussion of the ineffectiveness of § 605, see *infra* Part IV.A.1.

15. See *infra* Part III.B.

16. *Katz v. United States*, 389 U.S. 356, 356 (1967).

17. Elsewhere, I contend that privacy must be conceptualized in a multifaceted way, from the bottom-up by focusing on social practices rather than a rigid category with a single unifying essence or common denominator. See Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1088–99 (2002).

private, and therefore not protected by the Fourth Amendment.¹⁸ This conception of privacy is not responsive to life in the modern Information Age, where most personal information exists in the record systems of hundreds of entities. The Court has turned its back on one of the most far-reaching and potentially dangerous law enforcement practices of our times. Similar to the 40 years following *Olmstead*, the only form of regulatory control is statutory, which has thus far has been woefully inadequate.

In this Article, I contend that this state of affairs poses one of the most significant threats to privacy in the twenty-first century. The protection of privacy requires an “architecture of power.”¹⁹ This architecture represents the way that law structures social relationships. The law creates and constructs the world we live in by shaping an individual’s relationships with other individuals, institutions, and the government. Ideally, the law should establish an architecture of power to maintain an appropriate balance of power in these relationships. Such a balance is critical to dignity, self-fulfillment, freedom, democracy, and other fundamental values. In our highly bureaucratized world, personal information is an essential element of these relationships. Protecting privacy with an architecture of power involves erecting a legal structure for responding to the ever-increasing data flows of the Information Age. Beyond a set of individual rights, protecting privacy requires an architecture that regulates the way information may be collected and used.

The focus of this Article is on our relationships with the government. An architecture of power must address two fundamental problems of government. First, it should address how to control the population without stifling liberty, in other words, how to balance order and freedom. Second, it should determine how to control the government so that it remains accountable to the people. This includes preventing officials from abusing their power, and guarding against excessive growth in government power that threatens to override the power of the people. One of the most

18. See *infra* Part III.C.

19. Lawrence Lessig has popularized the term “architecture” to refer to technological systems of governance—the way that computer code structures what we can do and how we act in cyberspace. See generally, LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999) [hereinafter CODE]; Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56 (1999). I use this term more broadly than Lessig does, to refer to a particular power structure, not merely created by computer code or technology, but by the law. Although certainly not antagonistic to law, Lessig’s view of privacy privileges technological to legal architecture. According to Lessig, law merely sets the default entitlements to information, and technological architectures do the rest. See *id.* at 160–61. However, I believe that law has a much larger role to play in the protection of privacy. Solove, *supra* note 7, at 1445–55.

profound powers of the government is its machinery for enforcing the law, which increasingly requires personal information to function. Therefore, an architecture of power must be developed to regulate the flow of personal information between the private sector and the government. In this Article, I compare the architectures established by the Fourth Amendment to the current statutory regulatory regime, and articulate a theory identifying the types of architectural features that will create the appropriate balance between privacy and effective law enforcement.

In Part II, I describe the extensive records of personal information that are maintained by third parties and the rapidly increasing information flows between the government and private sector entities. I illustrate why these information flows present a serious threat to privacy and why an architecture of power is essential to ensure that privacy is adequately protected.

In Part III, I describe the basic architecture of power that the Fourth Amendment endeavors to establish and explain why this architecture has many important features for the effective protection of privacy. Specifically, I contend that the Fourth Amendment embodies a Madisonian theory of government that aims to balance government control with liberty while at the same time keeping government power under control. Substantively, it restricts searches and seizures through the reasonableness requirement and provides procedural safeguards through the warrant and probable cause requirements. These reflect the fractionalization of power among different government branches that James Madison believed was essential to restrain governmental power. I quarrel with a number of prominent critics who contend that the Fourth Amendment should not concern itself with protecting privacy. In the world of modern law enforcement, which has become significantly bureaucratized, privacy is an essential facet of the relationship between the government and the people. I explain at length why this is so, and defend the wisdom of the Fourth Amendment's architecture of power against its critics.

In Part IV, I critique the architecture of power created by the statutory regime that has filled the void left by the inapplicability of the Fourth Amendment to third party records. This architecture of power is a faulty one—uneven, overly complex, filled with gaps and loopholes, and containing numerous weak spots.

In Part V, I suggest guidelines for an appropriate architecture of power to regulate government access to personal information in third party record systems. Regarding the scope of the architecture, I develop a way to define

what types of government information gathering from third parties should be regulated. This is a particularly difficult question. Too broad of a scope could hinder legitimate law enforcement because criminal investigations often require the gathering of data from third parties. Since the type of information collection that raises concern involves data gathered from dossiers maintained in private sector entities, I recommend that the architecture should encompass all instances where third parties share personal data contained within a “system of records,” a term I borrow from the federal Privacy Act. Regarding the architecture’s structure, I explore a spectrum of procedural mechanisms to establish the delicate balance between privacy and law enforcement interests. I recommend a fusion of Fourth Amendment architecture and the architecture of subpoenas and court orders.

II. GOVERNMENT INFORMATION GATHERING AND THE PRIVATE SECTOR

A. THIRD PARTY RECORDS AND THE GOVERNMENT

We live in the early stages of the Information Age, a time when technology has given us unprecedented abilities to communicate, transfer and share information, access data, and analyze a profound array of facts and ideas. The complete benefits of the Information Age do not simply come to us. We must “plug in” to join in. In other words, we must establish relationships with a panoply of companies. To connect to the Internet, we must subscribe to an ISP, such as America Online (AOL) or Earthlink. To be able to receive more than a few television channels, we need to open an account with a cable company. Phone service, mobile phone service, and other utilities require us to open accounts with a number of entities.

Further, life in modern society demands that we enter into numerous relationships with professionals (doctors, lawyers, accountants), businesses (restaurants, video rental stores), merchants (bookstores, mail catalog companies), publishing companies (magazines, newspapers), organizations (charities), financial institutions (banks, investment firms, credit card companies), landlords, employers, and other entities (insurance companies, security companies, travel agencies, car rental companies, hotels). Our relationships with all of these entities generate records containing personal information necessary to establish an account and record of our transactions, preferences, purchases, and activities. We are becoming a society of records, and these records are not held by us, but by third parties.

In earlier times, communities were smaller and people knew each other's business. Today, the predominant mode of spreading information is not through the flutter of gossiping tongues but through the language of electricity, where information pulses between massive record systems and databases. From the standpoint of individual freedom, this development has both an upside and a downside. Individuals can more readily escape from the curious eyes of the community, freeing themselves from stifling social norms inhibiting individuality and creativity. On the other hand, an ever-growing series of records is created about almost every facet of a person's life.

These record systems are becoming increasingly useful to law enforcement officials. Personal information can help the government detect fraud, espionage, fugitives, smuggling cartels, drug distribution rings, and terrorist cells. Information about a person's financial transactions, purchases, and religious and political beliefs can assist law enforcement in investigating suspected criminals, individuals providing money and assistance to terrorists, or profiling people for more thorough searches at airports.²⁰

The government, therefore, has compelling reasons to obtain personal information found in records maintained by third parties that can reveal a myriad of details about a person. For instance, from pen registers and trap and trace devices, the government can obtain a list of all the phone numbers dialed to or from a particular location, potentially revealing the people with whom a person associates. From bank records, which contain one's account activity and check writing, the government can discover the various companies and professionals that a person does business with (ISP, telephone company, credit card company, magazine companies, doctors, attorneys, and so on).²¹ Credit card company records can reveal where one eats and shops and which cultural events one attends. The government can obtain one's travel destinations and activities from travel agent records. From hotel records, it can discover the numbers a person dialed and the pay-per-view movies a person watched.²² The government can potentially

20. See Robert O'Harrow, Jr., *Intricate Screening of Flyers In Works: Database Raises Privacy Concerns*, WASH. POST., Feb. 1, 2002, at A1.

21. See *Cal. Bankers Ass'n v. Shultz*, 416 U.S. 21, 85 (1974) (Douglas, J. dissenting) ("In a sense a person is defined by the checks he writes. By examining them the agents get to know his doctors, lawyers, creditors, political allies, social connections, religious affiliation, educational interests, the papers and magazines he reads, and so on *ad infinitum*.").

22. See Dana Hawkins, *Gospel of a Privacy Guru: Be Wary; Assume the Worst*, U.S. NEWS & WORLD REP., June 25, 2001, <http://www.usnews.com/usnews/nycu/tech/articles/010625/>

obtain one's thumbprint from car rental companies that collect them to investigate fraud.²³ From cable companies, the government can obtain a list of the special pay channels subscribed to or the various pay-per-view events a person has watched. From video stores, the government can access an inventory of the videos that a person has rented.

The government can also glean a wealth of information from the extensive records employers maintain about their employees.²⁴ Employers frequently monitor their employees.²⁵ Some use Internet filter software to track how employees surf the World Wide Web.²⁶ Employers often keep information about an employee's e-mail use, including back-up copies of the contents of e-mail. A number of employers also conduct drug testing,²⁷ and many require prospective employees to answer questionnaires asking about drug use, finances, mental health history, marital history, and sexuality.²⁸ Some even require prospective hires to take a psychological screening test.²⁹

Landlords are another fertile source of personal information. Landlord records often contain financial, employment, and pet information, in addition to any tenant complaints. Many landlords also maintain logbooks at the front desk where visitors sign in. Some apartment

tech/privacy.htm (describing hotel chain sharing lists of the movies, including pornographic ones, customers pay to watch in their hotel rooms).

23. Julia Scheeres, *No Thumbprint, No Rental Car*, WIRED NEWS, Nov. 21, 2001, at <http://wired.com/news/print/0,1294,48552,00.html>.

24. See, e.g., Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and the Fair Information Practices*, 2000 WISC. L. REV. 743, 770-71 (describing lack of employee privacy).

25. See Dana Hawkins, *Digital Skulduggery*, U.S. NEWS & WORLD REP., Oct. 2, 2000 at 64. For a detailed account of privacy in the workplace, see generally, JOHN D.R. CRAIG, *PRIVACY AND EMPLOYMENT LAW* (1999).

26. J.C. Conklin, *Under the Radar: Content Advisor Snoops as Workers Surf Web*, WALL ST. J., Oct. 15, 1998, at B8.

27. See *Baggs v. Eagle-Pitcher Indus., Inc.*, 750 F. Supp. 264, 272-73 (W.D. Mich. 1990) (holding no tort or contract remedies for at-will employee discharged for refusing to take a drug test). For an excellent discussion of the issue, see generally, Pauline T. Kim, *Privacy Rights, Public Policy, and the Employment Relationship*, 57 OHIO ST. L.J. 671 (1996).

28. This information was requested in employer questionnaires in *American Federation of Government Employees v. HUD*, 118 F.3d 786 (D.C. Cir. 1997) and *Walls v. City of Petersburg*, 895 F.2d 188 (4th Cir. 1990). The Americans With Disabilities Act (ADA), 42 U.S.C. § 12112 prevents inquiries of an applicant regarding disabilities; however, inquiries can be made "into the ability of an applicant to perform job related functions." 42 U.S.C. § 12112(d)(2)(B) (2002). An employer may require all entering employees to undergo a medical examination. § 12112(d)(3).

29. See Sarah Schafer, *Searching for a Workable Fit; Employers Try Psychological Tests to Help with More than the Right Hire*, WASH. POST, Jan. 14, 1999, at V5.

buildings use biometric identification devices, such as hand scanners, to control access to common areas such as gyms.

Increasingly, companies and entities that we have never established any contact with have dossiers about us. From credit reporting agencies, the government can glean information relating to financial transactions, debts, creditors, and checking accounts.³⁰ The government can also find out details about people's race, income, opinions, political beliefs, health, lifestyle, and purchasing habits from database companies, since many companies keep extensive personal information on millions of Americans.³¹ One database company maintains information about people's supermarket purchases, collected through the use of supermarket discount cards. This data can reveal a complete inventory of one's groceries, over-the-counter medications, hygiene supplies, and contraceptive devices, among others.³²

Beyond the records described above, the Internet has the potential to become one of the government's greatest information gathering tools.³³ There are two significant aspects of the Internet that make it such a revolutionary data collection device. First, it gives many individuals a false sense of privacy. The secrecy and anonymity of the Internet is often a mirage. People are rarely truly anonymous because ISPs keep records of a subscriber's screen name and pseudonyms.³⁴ ISP account information can also include the subscriber's name, address, phone numbers, passwords, information about web surfing sessions and durations, credit card and bank account information.³⁵ By learning a person's screen name, the government can identify the person behind the pseudonym postings to newsgroups or chatrooms. For example, in *McVeigh v. Cohen*,³⁶ AOL

30. See Solove, *Privacy and Power*, *supra* note 7, at 1408–09.

31. See *id.* at 1406–10.

32. Catalina Marketing Corp. has collected information about the supermarket purchases of thirty million households. See Robert O'Harrow, Jr., *Behind the Instant Coupons, a Data-Crunching Powerhouse*, WASH. POST., Dec. 31, 1998, at A20.

33. Although the rise of the Internet promises to herald a new age of freedom, there is a dark side to the Internet, where instead of a world of freedom, it is becoming a realm of domination and control. As Lawrence Lessig observes: "[C]yberspace does not guarantee its own freedom but instead carries an extraordinary potential for control." LESSIG, *CODE*, *supra* note 19, at 58.

34. See, e.g., *United States v. Hambrick*, 55 F. Supp. 2d 504, 505 (W.D. Va. 1999) (obtaining from ISP the identity of a pseudonymous individual in an Internet chat room); *United States v. Charbonneau*, 979 F. Supp. 1177, 1179 (S.D. Ohio 1997) (obtaining the identity of an pseudonymous Internet user from ISP); *State v. Schroeder*, 613 N.W.2d 911, 913 (Wis. Ct. App. 2000) (obtaining from ISP the identity of individual who posted sexually suggestive comments on the Internet about another individual).

35. See 18 U.S.C. § 2703(c) (2000), as amended by the USA-PATRIOT Act §§ 210–11.

36. 983 F. Supp. 215, 217 (D.D.C. 1998).

provided a Navy official with the identity of an individual using a pseudonym who indicated he was gay and worked in the military. Based on this information, the Navy proceeded to initiate discharge proceedings under the “Don’t Ask, Don’t Tell” policy.³⁷

A person’s ISP can also keep records about websurfing and e-mail activity. At the government’s request, an ISP can keep logs of the e-mail addresses with which a person corresponds. Further, the government can use ISP information to find out who uses a particular e-mail address. Thus, it can discover the identities of the individuals with whom a person corresponds. Further, if a person stores e-mail that is sent and received with the ISP, the government can obtain the contents of those e-mails.

Second, the Internet is unprecedented in the degree of detailed information that can be gathered and stored. It is one of the most powerful generators of records in human history. Jerry Kang notes that as we wander through cyberspace, a host of entities assemble information that is “detailed, computer-processable, indexed to the individual, and permanent.”³⁸ For example, as more information goes digital, and as copyright holders seek new ways to profit from their copyrights, the technological tools are in place to monitor the music people listen to and the books people read.³⁹

Websites often accumulate a great deal of information about their users. Through the use of a “cookie,” which identifies a user by deploying a text file into the user’s computer, websites can detect the previous website and parts of the site a user accessed.⁴⁰ This data is called “clickstream data” because it records nearly every click of the mouse.⁴¹ Another information collection device, known as a “web bug,” involves hidden pixel tags secretly planted on a user’s hard drive that surreptitiously

37. When he called AOL, the official did not identify himself as a Navy official but instead stated that he had received a fax from a pseudonymous individual and that he wanted to find out the identity of the individual. The AOL representative identified the individual.

38. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1199 (1998).

39. See Julie E. Cohen, *The Right to Read Anonymously: A Closer Look at “Copyright Management” in Cyberspace*, 28 CONN. L. REV. 981, 983 (1996) (“The same technologies that enable readers to access digitally stored works, however, also will enable copyright owners to generate precise and detailed records of such access.”); Schwartz, *Internet Privacy and the State*, *supra* note 6, at 849 (noting that copyright management “systems enable copyrighted works themselves to carry out a pervasive monitoring of individual activity”). See also Pamela Samuelson, *Will the Copyright Office Be Obsolete in the Twenty-First Century?*, 13 CARDOZO ARTS & ENT. L.J. 58 (1994).

40. See Solove, *Privacy and Power*, *supra* note 7, at 1411–12.

41. See *id.* at 1411.

gather data about the user.⁴² Websites also collect data when people fill out online questionnaires pertaining to their hobbies, health, and interests. Further, a person's Internet postings are archived and do not readily disappear.⁴³ As we invest more time on the Internet, strangers and unfamiliar organizations are keeping permanent records about our lives.

Thus, the government can glean a substantial amount of information about visitors to a particular website. For example, certain health websites ask individuals to fill out questionnaires about their symptoms to determine whether they have a disease.⁴⁴ Other websites have questionnaires relating to psychology and personality.⁴⁵ From Internet retailers, the government can learn about the books, videos, music, and electronics that one purchases. Some Internet retailers, such as "Amazon.com," record all the purchases a person makes throughout the many years that the person has been shopping on the website. Also, retailers use surveys to identify how a person rates books and videos.⁴⁶ Based on this information, the government can discover a consumer's interests, sexuality, political views, religious beliefs, and lifestyle. Further, if a person buys a gift from an Internet retailer and has it mailed to a friend, the government may learn the friend's name and address and develop a list of an individual's friends and acquaintances.

The government may also obtain information from websites that operate personalized home pages. Home pages enable users to keep track of the stocks they own, favorite television channels, airfares for favorite destinations, and news of interest.⁴⁷ Other websites, such as Microsoft Network's calendar service, allow users to maintain their daily schedule and appointments.⁴⁸ Further, there are some database companies that amass extensive profiles of people's websurfing habits.⁴⁹

42. See Robert O'Harrow, Jr., *Fearing a Plague of 'Web Bugs'; Invisible Fact-Gathering Code Raises Privacy Concerns*, WASH. POST, Nov. 13, 1999, at E1; Leslie Walker, *Bugs That Go Through Computer Screens*, WASH. POST, Mar. 15, 2001, at E1.

43. J.D. Lasica, *The Net NEVER Forgets*, SALON, Nov. 25, 1998, at <http://www.salon.com/21st/feature/1998/11/25feature.html>.

44. For a discussion of the types of information collected by health websites, see Pew Internet & American Life Project, *Exposed Online: Why the New Federal Health Privacy Regulation Doesn't Offer Much Protection to Internet Users* (Nov. 2001), at <http://www.pewinternet.org>.

45. *Id.*

46. This feature is available on Amazon.com at <http://www.amazon.com>.

47. For example, Yahoo!, at <http://www.yahoo.com>, offers a personalized web page service.

48. See <http://calendar.msn.com/CalendarNorm.html>.

49. See JIM STERNE, *WHAT MAKES PEOPLE CLICK: ADVERTISING ON THE WEB*, 238-41 (1997); Solove, *Privacy and Power*, *supra* note 7, at 1412.

While life in the Information Age has brought us a dizzying amount of information, it has also placed a profound amount of information about our lives in the hands of numerous entities. These digital dossiers are increasingly becoming digital biographies, a horde of aggregated bits of information combined to reveal a portrait of who we are based upon what we buy, the organizations we belong to, how we navigate the Internet, and which shows and videos we watch.⁵⁰ This information is not held by trusted friends or family members, but by large bureaucracies that we do not know very well or sometimes do not even know at all.

B. GOVERNMENT-PRIVATE SECTOR INFORMATION FLOWS

Information is becoming more fluid and more readily collected, stored, transferred, and combined with other information. This increasing movement of information is frequently called “information flow.”⁵¹ Elsewhere, I have discussed the problems of information flow among various private sector entities⁵² as well as from the government to the private sector.⁵³ There is another problematic type of information flow that is rapidly escalating—data transfers from the private sector to the government.

The government is increasingly contracting with private sector entities to acquire databases of personal information. Database firms are willing to supply the information and the government is willing to pay for it.⁵⁴ For example, the private sector company ChoicePoint, Inc. has multimillion dollar contracts with about thirty-five federal agencies including the Federal Bureau of Investigation (FBI) and the Internal Revenue Service (IRS) to provide personal information.⁵⁵ ChoicePoint’s database contains over ten billion records indexed by Social Security numbers. The information is gathered from public records, private detectives, credit reporting agencies, and other sources.⁵⁶

50. See Daniel J. Solove, *Access and Aggregation: Privacy, Public Records, and the Constitution*, 86 MINN. L. REV. (forthcoming 2002).

51. See generally Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315 (2000); Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497 (1995).

52. See generally Solove, *Privacy and Power*, *supra* note 7.

53. See generally Solove, *Access and Aggregation*, *supra* note 50.

54. FED. TRADE COMM’N, INDIVIDUAL REFERENCE SERVICES 1, 27–28 (1997), available at 1997 WL 784156, at *9.

55. See Glenn R. Simpson, *Big Brother-in-Law: If the FBI Hopes to Get the Goods on You, It May Ask ChoicePoint*, WALL ST. J., Apr. 13, 2001, at A1.

56. See *id.*

The Department of Defense allegedly has purchased information collected by a private sector company about students' web surfing habits.⁵⁷ Thus far, the agency has only obtained aggregate information, but in light of the events of September 11, there might be a strong interest in acquiring personally identifiable information about students' web searching habits because some of the terrorists posed as students.

A second form of information flow from the private sector to the government emerges when the government requests private sector records for particular investigations or compels their disclosure by subpoena or court order. Voluntary disclosure of customer information is within the third party company's discretion.⁵⁸ Further, whether a person is notified of the request and given the opportunity to challenge it in court is also within the company's discretion.⁵⁹

The September 11, 2001 terrorist attacks have changed the climate for private sector-to-government information flows. Law enforcement officials have a greater desire to obtain information that could be helpful in identifying terrorists or their supporters, including information about what people read, with whom they associate, their religion, and their lifestyle. Following the September 11 attack, the FBI simply has requested records from businesses without a subpoena, warrant, or court order.⁶⁰ Recently, Attorney General John Ashcroft has revised longstanding guidelines for FBI surveillance practices. Under the previous version, the FBI could monitor public events and mine the Internet for information only when "facts or circumstances reasonably indicate that a federal crime has been, is being, or will be committed."⁶¹ Under the revised version, the FBI can engage in these types of information gathering without any requirement that this gathering be part of a legitimate investigation or related in any manner to criminal wrongdoing.⁶² The FBI can now collect "publicly available information, whether obtained directly or through services or resources (whether nonprofit or commercial) that compile or analyze such

57. See Jeffrey Benner, *The Army is Watching Your Kid*, WIRED NEWS, Jan. 29, 2001, at <http://www.wired.com/news/print/0,1294,41476,00.html>.

58. See *infra* Part IV.

59. See *infra* Part IV.

60. Daniela Deane, *Legal Niceties Aside . . . ; Federal Agents Without Subpoenas Asking Firms for Records*, WASH. POST, Nov. 7, 2001, at E1.

61. THE ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND DOMESTIC SECURITY/TERRORISM INVESTIGATIONS § II.C.1 (March 21, 1989).

62. See THE ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND TERRORISM ENTERPRISE INVESTIGATIONS § VI (May 30, 2002).

information; and information voluntarily provided by private entities.”⁶³ Further, the FBI can “carry out general topical research, including conducting online searches and accessing online sites and forums.”⁶⁴

In conjunction with the government’s greater desire for personal information, the private sector has become more willing to supply it. Before September 11, the private sector, in certain circumstances, strongly opposed sharing information with the government. For example, when Independent Counsel Kenneth Starr subpoenaed a Washington, D.C. bookstore’s records of Monica Lewinsky’s purchases,⁶⁵ the store spent over \$100,000 in legal costs vigorously opposing the subpoena.⁶⁶ In March of 2000, the Tattered Cover, a bookstore in Denver, Colorado, contested a search warrant in order to protect its customers’ privacy.⁶⁷ Prior to September 11, an attorney for Amazon.com revealed that law enforcement officials informally requested information about book, music, and video purchases. Amazon.com “typically” informed law enforcement officials that it valued its customers’ privacy, it would not disclose their information, albeit with some exceptions.⁶⁸

September 11 changed these attitudes. Background check companies, for instance, experienced a large boost in business after September 11.⁶⁹ An Internet company shut down its free anonymous Internet surfing

63. *Id.*

64. *Id.* at VI.B.1. See also Susan Schmidt & Dan Eggen, *FBI Given More Latitude: New Surveillance Rules Remove Evidence Hurdle*, WASH. POST, May 30, 2002, at A1.

65. In particular, Starr was interested in discovering if Lewinsky had purchased Nicholson Barker’s *Vox*, a novel that pertained to phone sex. See Mike Feinsilber, *Bookstore Refuses to Comply with Starr’s Subpoena for Lewinsky Book List*, NANDO TIMES NEWS (1998), <http://archive.nandotimes.com/newsroom/nt/529nonono.html>.

66. See *id.*

67. Felicity Barringer, *Using Books as Evidence Against Their Readers*, N.Y. TIMES, Apr. 8, 2001, at WK3; Justin Rickard, *Police vs. Bookstore in Privacy Rights Case*, (Dec. 16, 2000), at <http://www.privacyfoundation.org/resources/bookstore.asp>. See also *Our Books Are Our Business*, ABCNEWS.COM, at http://my.abcnews.go.com/2020_020216_bookstores_feature.htm. The technique of obtaining information from bookstores has escalated since the *Monica Lewinsky* episode. In 2000–01, prior to September 11, Borders bookstores in Massachusetts and Kansas were searched and subpoenaed. See Barringer, *supra*, at WK3. In the *Tattered Cover* case, the Colorado Supreme Court recently sided with the bookstore. See *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044 (Colo. 2002).

68. Barringer, *supra* note 67.

69. Lisa Guernsey, *What Did You Do Before the War?*, N.Y. TIMES, Nov. 22, 2001, at G1. See also Victor Schachter & Trey Wichmann, *The Aftermath of September 11: No Longer Business as Usual for Security, Safety to Privacy in the Workplace*, in *THIRD ANNUAL INSTITUTE PRIVACY LAW: NEW DEVELOPMENTS & ISSUES IN A SECURITY CONSCIOUS WORLD* 623, 627 (Francoise Gilbert, John B. Kennedy & Paul M. Schwartz eds. 2002) (describing increase in employer scrutiny of applicants’ backgrounds).

service.⁷⁰ Several large financial companies developed agreements to provide information to federal law enforcement agencies.⁷¹

Indeed, in times of crisis or when serious crimes are at issue, the incentives to disclose information to the government are quite significant. Companies do not want to withhold information that will impede the investigation of a terrorist or murderer. They want to cooperate and help out.⁷²

When private sector entities refuse to cooperate, the government can compel production of the information by issuing a subpoena or obtaining a court order. As discussed in Part IV, these devices are very different from warrants because they offer little protection to the individual being investigated. Notification of the target of the investigation is often within the discretion of the third party.⁷³ Further, it is up to the third party to challenge the subpoena.⁷⁴ So, rather than spend the money and resources to challenge the subpoena, especially when the information is not valuable to their interests, companies can simply turn it over or permit the government to search their records.

Moreover, ISPs are integral to law enforcement officials' ability to investigate. Since September 11, AOL and Earthlink, two of the largest ISPs, have readily cooperated with the investigation of the terrorist attacks.⁷⁵ Often, ISPs have their own technology to turn over communications and information about targets of investigations. If they lack the technology, law enforcement officials can install devices such as "Carnivore" to locate the information.⁷⁶ Carnivore, now renamed to the more innocuous "DCS1000," is a computer program installed by the FBI at

70. Elinor Mills Abreu, *SafeWeb Shuts Free Anonymous Web Service*, INFOVAR.COM, Nov. 11, 2001, at http://www.infowar.com/class_1/01/class1_112001a_j.shtml.

71. See Paul Beckett, *Big Banks, U.S. Weigh Pooling Data on Terror*, WALL ST. J., Nov. 26, 2001, at A2; Robert O'Harrow, Jr., *Financial Database to Screen Accounts: Joint Effort Targets Suspicious Activities*, WASH. POST, May 30, 2002, at E1.

72. See David E. Rosenbaum, *A Nation Challenged: Questions of Confidentiality*, N.Y. TIMES, Nov. 22, 2001, at B7.

73. See *infra* Part IV.

74. See *infra* Part IV.

75. See Mike Snider, *Privacy Advocates Fear Trade-Off for Security; FBI Sends Warrants to Service Providers*, USA TODAY, Sept. 13, 2001, at D8.

76. See Robert Lemos, *FBI Taps ISPs in Hunt for Attackers*, ZD NET Sept. 12, 2001, at <http://zdnet.com/filters/printerfriendly/0,6061,5096919-2,00.html>.

an ISP.⁷⁷ It can monitor all ISP e-mail traffic and search for certain keywords in the content or headers of the e-mail messages.⁷⁸

These developments are troubling because private sector companies often have weak policies governing when information may be disclosed to the government. The privacy policy for the MSN network, an affiliation of several Microsoft, Inc. websites such as Hotmail (an e-mail service), Health, Money, Newsletters, eShop, and Calendar, states:

MSN Web sites will disclose your personal information, without notice, only if required to do so by law or in the good faith belief that such action is necessary to: (a) conform to the edicts of the law or comply with legal process served on Microsoft or the site. . . .⁷⁹

Though somewhat unclear, this privacy policy appears to require a subpoena or court order for the government to obtain personal data.

Amazon.com's privacy policy reads, "We release account and other personal information when we believe release is appropriate to comply with law . . . or protect the rights, property, or safety of Amazon.com, our users, or others."⁸⁰ It is unclear from this policy the extent to which Amazon.com, in its discretion, can provide information to law enforcement officials.

eBay, a popular online auction website, has a policy stating that [it] cooperates with law enforcement inquiries, as well as other third parties to enforce laws, such as: intellectual property rights, fraud and other rights. We can (and you authorize us to) disclose any information about you to law enforcement or other government officials as we, in our sole discretion, believe necessary or appropriate, in connection with an investigation of fraud, intellectual property infringements, or other activity that is illegal or may expose us or you to legal liability.⁸¹

This policy gives eBay almost complete discretion to provide the government with whatever information it deems appropriate.

Truste.com, a nonprofit organization providing a "trustmark" for participating websites that agree to abide by certain privacy principles, has drafted a model privacy statement that reads, "We will not sell, share, or

77. E. Judson Jennings, *Carnivore: U.S. Government Surveillance of Internet Transmissions*, 6 VA. J. L. & TECH. 10, ¶¶ 49, 96 (2001).

78. The USA-PATRIOT Act enshrined the FBI's Carnivore device into law. USA-PATRIOT Act § 216, codified at 18 U.S.C. § 3133(a)(3) (1994).

79. MSN Statement of Privacy, at <http://privacy.msn.com>.

80. Amazon.com Privacy Notice, at <http://www.amazon.com>.

81. Privacy Policy, at <http://pages.ebay.com/help/community/png-priv.html>.

rent [personal] information to others in ways different from what is disclosed in this statement.”⁸² This policy, however, does not contain any provision about supplying information to the government, and the quoted statement appears to be referring to other private sector entities such as marketers.⁸³ Further, the policy does not inform people that under existing law, information must be disclosed to the government pursuant to a subpoena or court order.⁸⁴

The government is also increasing information flow from the private sector by encouraging it to develop new information-gathering technologies. Private sector firms stand to profit from developing such technologies. Recently, private sector companies have expressed an eagerness to develop national identification systems and face-recognition technology.⁸⁵ In addition, the federal government has announced a “wish list” for new surveillance and investigation technologies.⁸⁶ Companies that invent such technologies can obtain lucrative government contracts.

The government has also funded private sector information-gathering initiatives. For instance, a company that began assembling a national database of photographs and personal information as a tool to guard against consumer fraud has received \$1.5 million from the Secret Service to aid in the development of the database.⁸⁷

In certain circumstances, where the private sector is not a willing collaborator with the government, new laws require their participation. For example, the Bank Secrecy Act of 1970 requires banks to maintain records of financial transactions to facilitate law enforcement needs, in particular, investigations and prosecutions of criminal, tax, or regulatory matters.⁸⁸ Congress passed the Act out of concern that the computerization of records would complicate white-collar crime prosecutions.⁸⁹ Under the Act, all federally insured banks must maintain records of each account holder’s financial transactions. Furthermore, the Secretary of the Treasury is

82. Model Privacy Statement, at http://truste.com/bus/pub_sample.html.

83. See *id.*

84. See *id.*

85. For example, Larry Ellison, the CEO of Oracle Corporation, proposed a system of national identification involving biometrics. See Larry Ellison, *Digital IDs Can Help Prevent Terrorism*, WALL ST. J., Oct. 8, 2001, at A26.

86. See Greg Schneider & Robert O’Harrow, Jr., *Pentagon Makes Rush Order for Anti-Terror Technology*, WASH. POST, Oct. 26, 2001, at A10.

87. Robert O’Harrow, Jr., *Drivers Angered over Firm’s Purchase of Photos*, WASH. POST, Jan. 28, 1999, at E1; Robert O’Harrow, Jr. & Liz Leyden, *U.S. Helped Fund Photo Database of Driver IDs: Firm’s Plan Seen as Way to Fight Identity Crime*, WASH. POST, Feb. 18, 1999, at A1.

88. 31 U.S.C. § 1081 (1994).

89. H. JEFF SMITH, *MANAGING PRIVACY* 24 (1994).

authorized to require that certain domestic financial transactions be reported to the government.⁹⁰ Under regulations promulgated by the Secretary of the Treasury, a bank must report every financial transaction in excess of \$10,000.⁹¹

In addition, Congress has passed the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 to assist with investigations of parents who do not pay child support. It requires that employers collect personal information from all new employees including Social Security numbers, addresses, and wages.⁹²

Congress has also passed the Communications Assistance for Law Enforcement Act (CALEA) of 1994,⁹³ which requires telecommunications service providers to develop technology to assist government surveillance of individuals.⁹⁴

All of this suggests that businesses and government have become allies. When their interests diverge, new laws requiring cooperation are passed. We are increasingly seeing collusion, partly voluntary, partly coerced, between the private sector and the government.

C. THE DANGERS OF GOVERNMENT INFORMATION GATHERING

Although there are certainly many legitimate needs for law enforcement officials to obtain personal data, there are also many dangers to unfettered government access to information. There are at least three general types of harms. The first has been discussed under the rubric of the "Big Brother metaphor."⁹⁵ Big Brother is the totalitarian government in George Orwell's *Nineteen Eighty-Four*, which achieved total domination by monitoring every facet of its citizens' private lives.⁹⁶ Although elsewhere it is suggested that the Big Brother metaphor does not capture the problem of the collection and use of personal information by private

90. 31 U.S.C. § 1081.

91. See 31 C.F.R. § 103.22(1). In *California Bankers Association v. Shultz*, 416 U.S. 21, 67–69 (1974), the Court held that the bankers lacked standing to challenge the regulations. *Shultz* effectively resolved the Fourth Amendment rights of the individuals with accounts at the bank. *Id.* According to the third party doctrine, these individuals have no reasonable expectation of privacy in their bank records. *Id.*

92. See Personal Responsibility and Work Opportunity Reconciliation Act of 1996, Pub. L. No. 104–193, 110 Stat. 2105 (1996). See generally Robert O' Harrow, Jr., *Uncle Sam Has All Your Numbers*, WASH. POST, June 27, 1999, at A1.

93. Pub. L. 103–414, 108 Stat. 4279 (1994).

94. See *United States Telecom Ass'n v. FCC*, 227 F.3d 450, 454 (D.C. Cir. 2000).

95. See Solove, *Privacy and Power*, *supra* note 7, at 1393.

96. See generally GEORGE ORWELL, *NINETEEN EIGHTY-FOUR* (1949).

sector entities,⁹⁷ it certainly remains persuasive in the context of government information-gathering. Indeed, historically, totalitarian governments have developed elaborate systems for collecting data about people's private lives.⁹⁸ Although the possibility of the rise of a totalitarian state is remote, if our society takes on certain totalitarian features, it could significantly increase the extent to which the government can exercise social control.

Second, government information-gathering can severely constrain democracy and individual self-determination. Paul Schwartz illustrates this with his theory of "constitutive privacy."⁹⁹ According to Schwartz, privacy is essential to both individuals and communities: "[C]onstitutive privacy seeks to create boundaries about personal information to help the individual and define terms of life within the community."¹⁰⁰ As a form of regulation of information flow, privacy shapes "the extent to which certain actions or expressions of identity are encouraged or discouraged."¹⁰¹ Schwartz contends that extensive government oversight over an individual's activities can "corrupt individual decision making about the elements of one's identity."¹⁰² Further, inadequate protection of privacy threatens deliberative democracy by inhibiting people from engaging in democratic activities.¹⁰³ This can occur unintentionally; even if government entities are not attempting to engage in social control, their activities can have collateral effects that harm democracy and self-determination.

For example, government information-collection interferes with an individual's freedom of association. The Court has held that there is a "vital relationship between freedom to associate and privacy in one's associations."¹⁰⁴ In a series of cases, the Court has restricted the government's ability to compel disclosure of membership in an organization.¹⁰⁵ In *Baird v. State Bar*,¹⁰⁶ for example, the Court has declared: "[W]hen a State attempts to make inquiries about a person's

97. See Solove, *Privacy and Power*, *supra* note 7, at 1417–19.

98. See Margaret Raymond, *Rejecting Totalitarianism: Translating the Guarantees of Constitutional Criminal Procedure*, 76 N.C. L. REV. 1193, 1198 (1998).

99. See Schwartz, *Privacy and Democracy in Cyberspace*, *supra* note 6, at 1658–59.

100. *Id.* at 1664.

101. *Id.* at 1665.

102. *Id.* at 1657.

103. See *id.* at 1651–52.

104. *NAACP v. Alabama*, 357 U.S. 449, 462 (1958).

105. See, e.g., *Shelton v. Tucker*, 364 U.S. 479, 489 (1960) (holding unconstitutional a law requiring teachers to disclose membership in organizations); *NAACP*, 357 U.S. at 466 (restricting compelled disclosure of membership lists of NAACP).

106. 401 U.S. 1 (1971).

beliefs or associations, its power is limited by the First Amendment. Broad and sweeping state inquiries into these protected areas . . . discourage citizens from exercising rights protected by the Constitution.”¹⁰⁷ The government’s extensive ability to glean information about one’s associations from third party records without any Fourth Amendment limitations seems to present an end-run around the principles articulated in these cases.¹⁰⁸

Extensive government information-gathering from third party records also implicates the right to speak anonymously. In *Talley v. California*,¹⁰⁹ the Court struck down a law prohibiting the distribution of anonymous handbills as a violation of the First Amendment. The Court held that “[p]ersecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all.”¹¹⁰ Further, the Court reasoned, “identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance.”¹¹¹ The Court reiterated its view of the importance of protecting anonymous speech in *McIntyre v. Ohio Elections Commission*.¹¹² The Court declared that “an author’s decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.”¹¹³ These cases, however, restricted the government from requiring individuals to identify themselves when speaking. With government information-gathering from third parties, namely ISPs, the government can readily obtain an anonymous or pseudonymous speaker’s identity. Only computer-savvy users can speak with more secure anonymity. When private parties attempt to obtain the identifying information, courts have held that subpoenas for this information must contain heightened standards.¹¹⁴ However, no such heightened standards apply when the *government* seeks to obtain the information.

107. *Id.* at 6.

108. It is unclear how receptive the Court will be to this argument. The Court has held that mere information gathering about a group’s public activities did not harm First Amendment interests enough to give rise to standing. *See Laird v. Tatum*, 408 U.S. 1, 12–15 (1972).

109. 362 U.S. 60, 63–64 (1960).

110. *Id.* at 64.

111. *Id.* at 65.

112. 514 U.S. 334, 334 (1995).

113. *Id.* at 342.

114. *See, e.g., Doe v. 2TheMart.com, Inc.*, 140 F.Supp.2d 1088, 1093–95 (W.D. Wash. 2001); *Columbia Insurance Co. v. Seescandy.com*, 185 F.R.D. 573, 578–80 (N.D. Cal. 1999).

Further, beyond typical anonymity is the ability to receive information anonymously. As Julie Cohen persuasively contends: "The freedom to read anonymously is just as much a part of our tradition, and the choice of reading materials just as expressive of identity, as the decision to use or withhold one's name."¹¹⁵ The lack of sufficient controls on the government's obtaining the extensive records about how individuals surf the web, the books and magazines they read, and the videos or television channels they listen to can implicate this interest.¹¹⁶

Additionally, the increasing information flow between the private sector and the government not only implicates the privacy of the target of an investigation, but can also affect the privacy of other individuals. The names, addresses, phone numbers, and a variety of data about a number of individuals can be ensnared in third party records pertaining to the target.

A third type of danger promoted by government information-gathering consists of the harms routinely arising in bureaucratic settings: decisions without adequate accountability, dangerous pockets of unfettered discretion, and choices based on short-term goals without consideration of the long-term consequences or the larger social effects. For example, this can lead to dangers such as hasty judgment in times of crisis, the disparate impact of law enforcement on particular minorities, cover-ups, petty retaliation for criticism, blackmail, framing, sweeping and disruptive investigations, racial, ethnic, or religious profiling, and so on. As David Garrow aptly observes:

I always had been much impressed by Joseph Conrad's message in *The Heart of Darkness*. I have come to feel, however, that the true nature of evil is much more akin to that described by Hannah Arendt than to

115. Cohen, *supra* note 39, at 1012.

116. Recently, the Colorado Supreme Court in *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044, 1044 (Colo. 2002), concluded that heightened scrutiny should apply to instances where police use a search warrant to seek records of a person's book purchases at bookstores. The holding was premised under Colorado's constitution:

We turn to our Colorado Constitution, which we now hold requires a more substantial justification from the government than is required by the Fourth Amendment of the United States Constitution when law enforcement officials attempt to use a search warrant to obtain an innocent, third-party bookstore's customer purchase records.

Id. at 1056. The court's holding was premised on a recognition that police searches of bookstores could chill bookstore customers' First Amendment rights to read anonymously: "When a person buys a book at a bookstore, he engages in activity protected by the First Amendment because he is exercising his right to read and receive ideas and information. Any governmental action that interferes with the willingness of customers to purchase books, or booksellers to sell books, thus implicates First Amendment concerns." *Id.* at 1052. The court concluded that "law enforcement officials must demonstrate a sufficiently compelling need for the specific customer purchase record sought from the innocent, third-party bookstore." *Id.* at 1058.

Conrad's horror. The danger we all face is not the consequences of man unbound from the restraints of society. It is the surrender of independent and critical judgment by people who work in large organizations. Evil is far more the product of people in complex institutions acting without personal reflection than it is something inherent in individual man.¹¹⁷

The most frequent problem is not that law enforcement agencies will be lead by corrupt and abusive leaders, although this arguably happened to some degree for nearly fifty years when J. Edgar Hoover directed the FBI.¹¹⁸ The problem is the risk that judgment will not be exercised in a careful and thoughtful manner. In other words, it stems from certain forms of government information-gathering shifting power toward a bureaucratic machinery that is poorly regulated and susceptible to abuse. This shift has profound social effects because it alters the balance of power between the government and the people, exposing individuals to a series of harms, increasing their vulnerability and decreasing the degree of power that they exercise over their lives.

As police forces grew in size, number, and technological surveillance capabilities, the relationship between government and citizen transformed. When the Fourth Amendment was ratified, organized police forces did not exist.¹¹⁹ Colonial policing was "[the] business of amateurs."¹²⁰ Sheriffs did not have a professional staff, and relied heavily on ordinary citizens to serve as constables or watchmen, whose primary duties consisted of patrolling rather than investigating.¹²¹ The government typically became involved in criminal investigations only after an arrest was made or a suspect was identified.¹²² In ordinary criminal cases, police rarely conducted searches prior to arrest.¹²³

Organized police forces developed during the nineteenth century, and by the middle of the twentieth century, policing reached an unprecedented level of organization and coordination.¹²⁴ At the center of the rise of

117. DAVID J. GARROW, *THE FBI AND MARTIN LUTHER KING, JR.* 18 (1980).

118. See generally CURT GENTRY, *J. EDGAR HOOVER: THE MAN AND THE SECRETS* (1991); RICHARD GID POWERS, *SECRECY AND POWER: THE LIFE OF J. EDGAR HOOVER* (1987).

119. See Silas J. Wasserstrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L.J. 19, 82 (1988); William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 408 (1995).

120. LAWRENCE M. FRIEDMAN, *CRIME AND PUNISHMENT IN AMERICAN HISTORY* 27 (1993).

121. Carol S. Steiker, *Second Thoughts About First Principles*, 107 HARV. L. REV. 820, 830-31 (1994).

122. See Stuntz, *supra* note 119, at 401.

123. See *id.*

124. See, e.g., FRIEDMAN, *supra* note 120, at 67; DAVID R. JOHNSON, *POLICING THE URBAN UNDERWORLD: THE IMPACT OF CRIME ON THE DEVELOPMENT OF THE AMERICAN POLICE 1800-1887*,

modern law enforcement was the development of the FBI. When the FBI was being formed in 1908, there was significant opposition in Congress to a permanent federal police force.¹²⁵ Members of Congress expressed trepidation over the possibility that such an investigatory agency could ascertain “matters of scandal and gossip” that could wind up being used for political purposes.¹²⁶ These concerns related to the potential dangers of the agency’s information-gathering capabilities, and as will be discussed later, the fears became realities during the course of the FBI’s history.

Today, we live in an endless matrix of law and regulation, administered by a multitude of vast government bureaucracies. Like most everything else in modern society, law enforcement has become bureaucratized.¹²⁷ There are large police departments armed with sophisticated technology that coordinate with each other.¹²⁸ There are massive agencies devoted entirely to investigation and intelligence. As William Stuntz notes, “The problem of discretionary, suspicionless searches and seizures in ordinary criminal cases is an incident of organized police forces—of a system that gives to police officers the job of investigating crimes, identifying suspects, and choosing which suspects to pursue.”¹²⁹

Many factors make it difficult for law enforcement officials to strike the delicate balance between order and liberty. Among them, there are tremendous pressures on law enforcement agencies to capture criminals, solve notorious crimes, keep crime under control, and prevent acts of violence and terrorism. This highly stressful environment can lead to short cuts, bad exercises of discretion, or obliviousness and insensitivity to people’s freedom. One of the most crucial aspects of keeping government power under control is a healthy scrutiny. Most law enforcement officials, however, are unlikely to view themselves with distrust and skepticism.

at 9 (1979); ERIC MONKKONEN, *POLICE IN URBAN AMERICA, 1860–1920*, at 42–44 (1981); Stuntz, *supra* note 119, at 435.

125. GENTRY, *supra* note 118, at 112. The organization created in 1908 was called the Bureau of Investigation (BI); it became the FBI in 1935. *See id.* at 113.

126. *Id.* at 111–12.

127. *See, e.g.*, Albert J. Reiss, Jr., *Police Organization in the Twentieth Century*, in *MODERN POLICING* 51, 68–82 (Michael Tonry & Norval Morris eds., 1992). Reiss points out that one of the distinctive and unique facets of law enforcement bureaucracy in the United States “is that the greatest discretionary powers are lodged with the lowest-ranking officials in the system and that most discretionary decisions are not made a matter of record.” *Id.* at 74.

128. *See, e.g.*, WHITFIELD DIFFIE & SUSAN LANDAU, *PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION* 118 (1998) (“Police forces today not only have access to nationwide (and often worldwide) records, but much of that access is directly available to officers in the field.”).

129. *See* Stuntz, *supra* note 119, at 408.

Police and prosecutors are too enveloped in the tremendous responsibilities and pressures of their jobs to maintain an unbiased and balanced perspective.

In short, one need not fear the rise of a totalitarian state or the inhibition of democratic activities to desire strong controls on the power of the government in collecting personal information. Specifically, government information-gathering must be regulated for a number of reasons.

First, by obtaining private sector records, the government can conduct the type of “fishing expeditions” that the Framers feared.¹³⁰ The government can increasingly amass vast dossiers on millions of individuals, conduct sweeping investigations, and search for vast quantities of information from a wide range of sources, without any probable cause or particularized suspicion. Information is easier to obtain, and it is becoming more centralized. Our digital dossiers are beginning to resemble digital biographies that are increasingly flowing to the government. As Justice Douglas noted in his dissent when the Court upheld the constitutionality of the Bank Secrecy Act:

These [bank records] are all tied to one’s social security number; and now that we have the data banks, these other items will enrich that storehouse and make it possible for a bureaucrat—by pushing one button—to get in an instant the names of the 190 million Americans who are subversives or potential and likely candidates.¹³¹

Second, as more private sector data becomes available to the government, there could be a de facto national database, or a large database of “suspicious” individuals.¹³² Federal governmental entities have conducted substantial information-gathering efforts on political groups throughout the twentieth century. From 1940 through 1973, for example, the FBI and CIA conducted a secret domestic intelligence operation, reading the mail of thousands of citizens.¹³³ The FBI’s investigations extended to members of the women’s liberation movement and prominent critics of the Vietnam War, and the FBI obtained information about

130. It is virtually undisputed that one of the central reasons the Framers created the Fourth Amendment was to guard against the use of general warrants. See, e.g., LEONARD W. LEVY, ORIGINS OF THE BILL OF RIGHTS 158 (1999); Tracey Maclin, *When the Cure for the Fourth Amendment Is Worse than the Disease*, 68 S. CAL. L. REV. 1, 9 (1994).

131. *California Bankers Ass’n v. Shultz*, 416 U.S. 21, 85 (1974) (Douglas, J. dissenting).

132. For a discussion of the harms of a national identification system, see Richard Sobel, *The Degradation of Political Identity Under a National Identification System*, 8 B.U. J. SCI. & TECH. L. 37 (2002). See also Solove, *Access and Aggregation*, *supra* note 50.

133. *DIFFIE & LANDAU*, *supra* note 128, at 138.

personal and sexual relationships that could be used to discredit them.¹³⁴ During the McCarthy era and the 1980s, the FBI sought information from libraries about the reading habits of certain individuals.¹³⁵ Between 1967 and 1970, the U.S. Army conducted wide-ranging surveillance, amassing extensive personal information about a broad group of individuals.¹³⁶ The impetus for the Army's surveillance was a series of riots that followed Dr. Martin Luther King, Jr.'s assassination.¹³⁷ The information collected involved data about finances, sexual activity, and health.¹³⁸ In 1970, Congress significantly curtailed the Army's program, and the records of personal information were eventually destroyed.¹³⁹ The danger of these information-gathering efforts is not only that it chills speech or threatens lawful protest, but also that it makes people more vulnerable by exposing them to potential future dangers such as leaks, security lapses, and improper arrests. For example, during the late 1960s and early 1970s, the Philadelphia Police Department (PPD) compiled about 18,000 files on various dissident individuals and groups. During a national television broadcast, PPD officials disclosed the names of some of the people on whom files were kept.¹⁴⁰

Third, government entities are using personal information in databases to conduct automated investigations. In 1977, in order to detect fraud, the federal government began matching its computer employee records with those of people receiving federal benefits.¹⁴¹ With the use of computers to match records of different government entities, the government investigated millions of people. Some matching programs used data obtained from private sector sources (merchants and marketing companies) to discover tax, welfare, and food stamp fraud as well as to identify drug couriers.¹⁴² Computer matching raised significant concerns, and in 1988,

134. See *id.* at 143.

135. See *id.* at 146; Barringer, *supra* note 67, at WK3.

136. See *DIFFIE & LANDAU*, *supra* note 128, at 143.

137. Although the Army's surveillance efforts were challenged before the Supreme Court on First Amendment grounds in *Laird v. Tatum*, 408 U.S. 1, 1 (1972), the Court concluded that the targets of the information gathering lacked standing because they only alleged "generalized yet speculative apprehensiveness that the Army may at some future date misuse the information in some way that would cause direct harm to [them]." *Id.* at 13.

138. *Id.*

139. See *id.* at 7.

140. See *Philadelphia Yearly Meeting of the Religious Society of Friends v. Tate*, 519 F.2d 1335, 1335 (3d Cir. 1975).

141. See PRISCILLA M. REGAN, *LEGISLATING PRIVACY* 86 (1995); Robert Gellman, *Does Privacy Law Work?*, in *TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE* 193, 198 (Philip E. Agre & Marc Rotenberg, eds., 1997).

142. See GARY T. MARX, *UNDERCOVER: POLICE SURVEILLANCE IN AMERICA* 209-10 (1988).

Congress finally passed a law regulating this practice.¹⁴³ The law has been strongly criticized as providing scant substantive guidance and having little practical effect.¹⁴⁴ This type of automated investigation is troubling because it alters the way that government investigations typically take place. Usually, the government has some form of particularized suspicion, a factual basis to believe that a particular person may be engaged in illegal conduct. Particularized suspicion keeps the government's profound investigative powers in check preventing widespread surveillance and snooping into the lives and affairs of all citizens. Computer matches, Priscilla Regan contends, investigate everyone, and most people who are investigated are innocent.¹⁴⁵

With the new information supplied by the private sector, there is an increased potential for more automated investigations, such as searches for all people who purchase books about particular topics or those who visit certain websites, or perhaps even people whose personal interests fit a profile for those likely to engage in certain forms of criminal activity. Automated investigations based on profiles share the problems experienced with profiling: the inappropriate use of stereotypes, race, and religion. Profiling or automated investigations based on information gathered through digital dossiers results in targets being inappropriately singled out for more airport searches, police investigations, or even arrest or detention.

Fourth, the government can use dossiers of personal information in mass roundups of distrusted or suspicious individuals whenever the political climate is ripe. As Pamela Samuelson observed: "One factor that enabled the Nazis to efficiently round up, transport, and seize assets of Jews (and others they viewed as 'undesirables') was the extensive repositories of personal data available not only from the public sector but

143. See Computer Matching and Privacy Protection Act (CMPPA) of 1988, Pub. L. No. 100-503, 102 Stat. 2507, *codified as amended at* 5 U.S.C. §§ 552a(a)(8)–(13), e(12), (o)–(r), (u). The CMPPA requires agencies to formulate procedural agreements before exchanging computerized record systems and establishes Data Integrity Boards within each agency. See *id.* The CMPPA establishes Data Integrity Boards within each agency to oversee matching, requires agencies to perform a cost-benefit analysis of proposed matching endeavors, and requires agencies to notify individuals of the termination of benefits due to computer matching and to permit individuals an opportunity to refute the termination. See *id.*

144. See GEN. ACCOUNTING OFFICE, COMPUTER MATCHING: QUALITY OF DECISIONS AND SUPPORTING ANALYSES LITTLE AFFECTED BY 1988 ACT (1993); SCHWARTZ & REIDENBERG, *supra* note 5, at 101; INFORMATION POLICY COMMITTEE, NATIONAL INFORMATION INFRASTRUCTURE TASK FORCE, OPTIONS FOR PROMOTING PRIVACY ON THE NATIONAL INFORMATION INFRASTRUCTURE: DRAFT FOR PUBLIC COMMENT 15 (Apr. 1997); Schwartz, *Privacy and Participation*, *supra* note 5, at 588 (noting that CMPPA "creates no substantive guidelines to determine when matching is acceptable").

145. See REGAN, *supra* note 141, at 90.

also from private sector sources.”¹⁴⁶ In the United States, information gathering greatly assisted the roundups of disfavored groups, including Japanese-Americans during World War II. Following the bombing of Pearl Harbor on December 7, 1941, the FBI detained thousands of Japanese-American community leaders in internment camps.¹⁴⁷ These initial roundups were facilitated by an index of potentially subversive people of Japanese descent compiled by the Justice Department beginning in the late 1930s.¹⁴⁸ In 1942, in the name of national security, about 120,000 people of Japanese descent living on the West Coast were imprisoned in internment camps.¹⁴⁹ The Census Bureau prepared special tabulations of Japanese-Americans, which, according to a 1942 War Department report, “became the basis for the general evacuation and relocation plan.”¹⁵⁰

The gathering of personal data also facilitated the Palmer Raids of 1919–20 (also known as the “Red Scare”). In 1991, a rash of bombings sparked the Palmer Raids, one of which damaged the home of Attorney General A. Mitchell Palmer.¹⁵¹ Bombs went off in eight other cities shortly thereafter and letter bombs were mailed to many elites.¹⁵² In a climate rife with fear of “Reds,” anarchists, and labor unrest,¹⁵³ Congress tasked the Bureau of Investigation (again, the organization that later became the FBI in 1935) with addressing these terrorist threats.¹⁵⁴ Under the direction of a young J. Edgar Hoover, the Bureau of Investigation developed an extensive index of hundreds of thousands of radicals.¹⁵⁵ This data was used to conduct a massive series of raids, in which over 10,000 individuals suspected of being Communists were rounded up, many without

146. Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1143 (2000). See also DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 373–74 (1989).

147. ERIC. K. YAMAMOTO, MARGARET CHON, CAROL I. IZUMI, JERRY KANG, & FRANK H. WU, RACE, RIGHTS, AND REPARATIONS: LAW AND THE JAPANESE AMERICAN INTERNMENT 38 (2001).

148. See *id.* at 96.

149. See *id.* at 38–39. See also Daniel J. Solove, *The Darkest Domain: Deference, Judicial Review, and the Bill of Rights*, 84 IOWA L. REV. 941, 941 (1999). See generally Eugene V. Rostow, *The Japanese American Cases—A Disaster*, 54 YALE L.J. 489 (1945).

150. DIFFIE & LANDAU, *supra* note 128, at 138. See also DAVID BURNHAM, THE RISE OF THE COMPUTER STATE 24 (1983).

151. FRANK J. DONNER, THE AGE OF SURVEILLANCE: THE AIMS AND METHODS OF AMERICA’S POLITICAL INTELLIGENCE SYSTEM 33 (1980).

152. See GENTRY, *supra* note 118, at 76. Most of the letter bombs were halted at the Post Office due to inadequate postage. See *id.*

153. See CHARLES H. MCCORMICK, SEEING REDS: FEDERAL SURVEILLANCE OF RADICALS IN THE PITTSBURGH MILL DISTRICT, 1917–1921, 120 (1997); POWERS, *supra* note 118, at 69.

154. See MCCORMICK, *supra* note 153, at 103.

155. See DONNER, *supra* note 151, at 34; GENTRY, *supra* note 118, at 79; POWERS, *supra* note 118, at 68.

warrants.¹⁵⁶ The raids resulted in a number of deportations, many based solely on membership in certain organizations.¹⁵⁷ When prominent figures in the legal community such as Roscoe Pound, Felix Frankfurter, and Zechariah Chafee, Jr., criticized the raids, Hoover began assembling a dossier on each of them.¹⁵⁸

Additionally, personal information gathered by the FBI enabled the extensive hunt for Communists during the late 1940s and 1950s—a period of history that has since been criticized as a severe over-reaction, resulting in the mistreatment of numerous individuals, and impeding the reform agenda begun in the New Deal.¹⁵⁹ According to Ellen Schrecker, federal agencies’ “bureaucratic interests, including the desire to present themselves as protecting the community against the threat of internal subversion, inspired them to exaggerate the danger of radicalism.”¹⁶⁰ Senator Joseph R. McCarthy, the figure who symbolized the anti-Communist movement, received substantial assistance from Hoover, who secretly released information about suspected Communists to McCarthy.¹⁶¹ Further, the FBI supplied a steady stream of names of individuals to be called before the House Un-American Activities Committee (HUAC).¹⁶² As Richard Powers observed, “information derived from the [FBI’s] files was clearly the lifeblood of the Washington anti-communist establishment.”¹⁶³ The FBI also leaked information about suspected individuals to employers and the press.¹⁶⁴ Public accusations of being a Communist carried an immense stigma and often resulted in a severe public backlash.¹⁶⁵ Individuals exposed as Communists faced retaliation in the private sector. Numerous journalists, professors and entertainers were fired from their jobs and blacklisted from future employment.¹⁶⁶

156. See GENTRY, *supra* note 118, at 93.

157. See POWERS, *supra* note 118, at 79–80.

158. See GENTRY, *supra* note 118, at 98–99.

159. See ELLEN SCHRECKER, *THE AGE OF MCCARTHYISM: A BRIEF HISTORY WITH DOCUMENTS* 92–94 (1994).

160. *Id.* at 10.

161. GENTRY, *supra* note 118, at 378–80, 402; POWERS, *supra* note 118, at 320–21.

162. See SCHRECKER, *supra* note 159, at 76–84. For further background about the McCarthy era, see generally ALBERT FRIED, *MCCARTHYISM: THE GREAT AMERICAN RED SCARE: A DOCUMENTARY HISTORY* (1997) and RICHARD M. FRIED, *NIGHTMARE IN RED: THE MCCARTHY ERA IN PERSPECTIVE* (1990).

163. POWERS, *supra* note 118, at 321.

164. See SCHRECKER, *supra* note 159, at 77.

165. See Seth I. Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1, 13–71 (1991).

166. SCHRECKER, *supra* note 159, at 76–84.

In short, government entities have demonstrated substantial abilities to gather and store personal information. Combined with the extensive data available about individuals in third party records, this creates a recipe for similar or greater government abuses in the future.

Fifth, unscrupulous government and law enforcement officials can abuse the availability of personal information databases. Recently, a Michigan State Police official allegedly accessed the Law Enforcement Information Network (LEIN), a law enforcement database of personal information, to examine her ex-husband's girlfriend's background.¹⁶⁷ The official was punished with a mere day's suspension without pay.¹⁶⁸ Prior to this incident, allegedly over ninety law enforcement officials had abused the LEIN during the past five years.¹⁶⁹

Sixth, information obtained by the government for one purpose can readily be used for another. For example, the government may be investigating whether a prominent critic of the war against terrorism has in any way assisted terrorists or is engaged in terrorism. In tracking an individual's activities, the government does not discover any criminal activity with regard to terrorism, but discovers that a popular website for downloading music files has been visited and that copyright laws have been violated.¹⁷⁰ Such information may ultimately be used to prosecute copyright violations as a pretext for the government's distaste for the individual's political views and beliefs. Further, dossiers maintained by law enforcement organizations can be selectively leaked to attack critics.¹⁷¹

Indeed, it is not far-fetched for government officials to amass data for use in silencing or attacking enemies, critics, undesirables, or radicals. For example, J. Edgar Hoover accumulated an extensive collection of files with detailed information about the private lives of numerous prominent individuals, including presidents, members of Congress, Supreme Court

167. See M.L. Elrick, *Cops Abuse Database, 3 Privacy Suits Say They Charge Officers Use LEIN to Check Out Personal Matters*, DETROIT FREE PRESS, Dec. 25, 2001, at A1.

168. See *id.*

169. See *id.*

170. For an excellent discussion of Napster and the impact of copyright law on music sharing, see generally Raymond Shih-Ray Ku, *The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology*, 69 U. CHI. L. REV. 263 (2002).

171. See JOSEPH BENSMAN & ROBERT LILIENTHAL, BETWEEN PUBLIC AND PRIVATE: THE LOST BOUNDARIES OF THE SELF 97 (1979) ("Large-scale organizations tend to invade privacy . . . in order to use the information so gained as a private means to secure its public goals and in part by using managed leaks to reveal the private vices of their organizational and personal enemies.").

justices, celebrities, civil rights leaders, and attorney generals.¹⁷² Hoover's data often included sexual activities.¹⁷³

We live in a world of mixed and changing motives. Data that is obtained for one purpose can be used for an entirely different purpose as motives change. For example, for several years, the FBI extensively wiretapped Martin Luther King, Jr.¹⁷⁴ They wiretapped his home, his office, and the hotel rooms that he stayed at when traveling.¹⁷⁵ Based on the wiretaps, the FBI learned of his extensive partying, extramarital affairs, and other sexual activities.¹⁷⁶ A high level FBI official even anonymously sent him a tape with highlights of the FBI's recordings along with a letter that stated:

King, there is only one thing left for you to do. You know what it is. You have just 34 days in which to do (this exact number has been selected for a specific reason, it has definite practical significant [sic]). You are done. There is but one way out for you. You better take it before your filthy, abnormal fraudulent self is bared to the nation.¹⁷⁷

Hoover's motive is disputed. One theory is that King was wiretapped because he was friendly with a person who had previously been a member of the Communist Party.¹⁷⁸ Another theory is that Hoover despised King. Hoover's longstanding hatred of King is evidenced by Hoover's nasty public statements about King, such as calling King "the most notorious liar" in the nation.¹⁷⁹ This was probably due, in part, to King's criticism of the FBI for failing to address adequately the violence against blacks in the South, Hoover's overreaction to any criticism of the FBI, and the FBI's practice of consistently targeting its critics.¹⁸⁰ As David Garrow hypothesizes, the original reason that the FBI began gathering information about King was due to fears of Communist ties; however, this motivation

172. CHARLES J. SYKES, *THE END OF PRIVACY: PERSONAL RIGHTS IN THE SURVEILLANCE SOCIETY* 160 (1999). See *DIFFIE & LANDAU*, *supra* note 128, at 163 (wiretapping of members of Congress and Supreme Court Justices); *GENTRY*, *supra* note 118 (providing detailed description of Hoover's collection of files and extensive wiretapping).

173. See *GARROW*, *supra* note 117, at 165.

174. See, e.g., *DIFFIE & LANDAU*, *supra* note 128, at 140–42. It was not until 1975, nearly a decade after the wiretapping and three years after Hoover's death, that Congress conducted an inquiry into the wiretapping of King through the famous Church Committee. See *id.* at 178.

175. *GARROW*, *supra* note 117, at 100–01.

176. See *id.* at 102 *passim*.

177. *Id.* at 126.

178. *Id.* at 26.

179. See *id.* at 78. Hoover's dislike of King may have also stemmed from racism. It is well-documented that Hoover was racist. See *id.* at 153.

180. See *id.* at 79–83.

changed once these fears proved unfounded and several powerful individuals at the FBI expressed distaste for King's sexual activities and moral behavior.¹⁸¹

D. PROTECTING PRIVACY WITH AN ARCHITECTURE OF POWER

The dangers discussed above illustrate why privacy is integral to freedom in the modern state. Privacy must be protected by establishing an architecture of power. The word "architecture" emphasizes that the protection of privacy must be achieved through establishing a particular social structure that distributes power in our various relationships.

Certain kinds of legal regulation can be readily analogized to architecture. Typically, we view architecture as the design of buildings and edifices. Buildings structure the way people feel and interact; they form and shape human relationships.¹⁸² Neal Kumar Katyal provides a fascinating account of how physical architecture—the way that neighborhoods and buildings are designed—can affect criminal behavior.¹⁸³ Law resembles architecture in many respects, especially in the way that certain forms of regulation affect social practices.

If we think of law as creating a structure, we can better understand the different forms that modern regulation must take to protect liberty in the modern state. We have freedom not simply because we have rights. Our liberty is constructed by various regulatory structures that regulate the safety of the products we buy, the conditions of the apartments we live in, the way that companies must interact with us, and the sanctity of the environment, among others. An architecture of power protects a number of social practices of which privacy forms a significant part. It protects

181. See *id.* at 151. According to Garrow, the investigation and electronic surveillance of King in 1962–63 began as an inquiry into King's ties with Levison; in 1963–64, the investigation turned to an effort to discredit and attack King.

182. See generally THOMAS A. MARKUS, *BUILDINGS AND POWER: FREEDOM AND CONTROL IN THE ORIGIN OF MODERN BUILDING TYPES* (1993). One of the most famous examples of the way architecture can affect social structure is the Panopticon, an architectural design for a prison developed by Jeremy Bentham. According to this design, prison cells are arranged around a central observation tower, from which all cells are visible. However, those in the cells cannot observe if anybody is in the tower. The goal of this architecture is for each prisoner to believe that at any moment, she could be being watched, and this belief will result in increased obedience. As Michel Foucault aptly noted, the Panopticon can be replicated in our society in ways not merely limited to physical architecture. Panoptic architecture can be part of the structure of social relationships. See MICHEL FOUCAULT, *DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON* 200–05 (Alan Sheridan Trans. 1977).

183. Neal Kumar Katyal, *Architecture as Crime Control*, 111 Yale L.J. 1039 (2002).

privacy by providing a regulatory structure that shapes relationships and safeguards individual liberties.

At the center of my view is the fact that privacy is an aspect of social practices, which involve relationships with other people and entities.¹⁸⁴ The need for privacy emerges from *within* a society, from the various social relationships that people form with each other, with private sector institutions, and with the government. We do not need privacy on a deserted island; rather, the need for privacy is engendered by the existence of society, from the fact that we must live together.

Relationships involve some balance of power between the parties. Power is not necessarily a zero-sum good, where more power to one party necessarily means less to another. However, certain configurations of power in these relationships have profound effects on the scope and extent of freedom, democracy, equality, and other important values. In the modern world, we are increasingly finding ourselves in a new type of relationship with public and private institutions. These relationships are different because our institutions are more bureaucratic in nature. Bureaucracies use more information and often exercise power over people through the use of personal data. Collecting and using personal information are having an intensifying influence on the effects of power in our social relationships. Therefore, protecting privacy is critical to governing these relationships, and consequently, to regulating the tone and tenor of life in the Information Age.

Protecting privacy through an architecture of power differs from protecting it as an individual right. Privacy is often viewed as an *individual* right.¹⁸⁵ It is seen as an individual possession, and its value is defined in terms of its worth to the individual. This view is severely flawed. John Dewey astutely critiqued the “conception of the individual as something given, complete in itself, and of liberty as a ready-made possession of the

184. For an extensive discussion of how privacy relates to social practices, see Solove, *supra* note 17, at 1126–43.

185. See, e.g., *Minnesota v. Carter*, 525 U.S. 83, 99 (1998) (Kennedy, J., concurring) (“Fourth Amendment protection . . . is in essence a personal right.”); *Whalen v. Roe*, 429 U.S. 589, 599–00 (1977) (privacy is an “individual interest in avoiding disclosure of personal matters”); Restatement (Second of Torts) § 652(I) comment (a) (stating that “[t]he right protected by the action for invasion of privacy is a personal right, peculiar to the individual whose privacy is invaded”); ELLEN ALDERMAN & CAROLINE KENNEDY, *THE RIGHT TO PRIVACY* xv (1995) (noting that “privacy is, by definition, a personal right”); William M. Beaney, *The Right to Privacy and American Law*, 31 LAW & CONTEMP. PROBS. 253, 254 (1966) (observing that “[t]he right to privacy is an affirmation of the importance of certain aspects of the individual person and his desired freedom from unreasonable intrusive conduct by others”).

individual, only needing the removal of external restrictions in order to manifest itself.”¹⁸⁶ According to Dewey, the individual is inextricably connected to society,¹⁸⁷ and rights are not immutable possessions of individuals, but are instrumental in light of “the contribution they make to the welfare of the community.”¹⁸⁸ The problem with viewing rights in purely individualistic terms is that it pits individual rights against the greater good of the community, with the interests of society often winning out because of their paramount importance when measured against one individual’s freedom.

Viewing privacy as an individual right against government information-gathering conceives of the harm to privacy as emanating from the invasion into the lives of particular people. But many of the people asserting a right to privacy against government information-gathering are criminals or terrorists, people we do not have a strong desire to protect. In modern Fourth Amendment law, privacy protection is often initiated at the behest of specific individuals, typically those accused of crimes. Often these individuals’ rights conflict with the need for effective law enforcement and the protection of society. Why should one individual’s preference for privacy trump the social goals of security and safety? This question is difficult to answer if privacy is understood as a right possessed by particular people.

In contrast, an architecture of power protects privacy differently and is based on a different conception of privacy. Privacy is not merely a right possessed by individuals, but is a form of freedom built into the social structure. It is thus an issue about the common good as much as it is about individual rights. It is an issue about social architecture, about the relationships that form the structure of our society.

Government information-gathering is a central facet of our relationships to the government. The increased stores of personal information in the hands of law enforcement officials pose a number of dangers, discussed in the previous section. The abuses of government information-gathering chronicled earlier could be dismissed as those generated by the megalomania of a few rogue officials. David Garrow has another theory, one that is more frightening. According to Garrow, the FBI

186. John Dewey, *The Future of Liberalism*, in 11 *LATER WORKS* 290 (Jo Ann Boydston ed. 1991).

187. See, e.g., JOHN DEWEY, *EXPERIENCE AND NATURE* 162–63 (1925); DEWEY, *LIBERALISM AND SOCIAL ACTION* 7 (1935).

188. John Dewey, *Liberalism and Civil Liberties*, in 11 *LATER WORKS* 374 (Jo Ann Boydston ed. 1991).

that targeted Martin Luther King, Jr. was not a “deviant institution in American society, but actually a most representative and faithful one.”¹⁸⁹ In other words, the FBI reflected the mindset of many Americans embodying all the flaws of that mindset. We like to blame individuals, and certainly the particular abusers are worthy of blame, but we cannot overlook the fact that the causes of abuse often run deeper than the corrupt official. Abuse is made possible by a bureaucratic machinery that is readily susceptible to manipulation. Thus, the problem lies in institutional structures and architectures of power. In the latter half of the twentieth century, and continuing to the present, one of the aspects of this architecture has been the lack of control over government information-gathering.

What is the most effective architecture of power to structure the way that the government can access personal information held by third parties? In the pages that follow, I discuss the two relevant architectures, that of the Fourth Amendment, which the Court has concluded does not apply to information held by third parties, and that of the statutory regime that has arisen in the void left by the inapplicability of the Fourth Amendment.

III. THE FOURTH AMENDMENT, RECORDS, AND PRIVACY

A. THE ARCHITECTURE OF THE FOURTH AMENDMENT

1. The Purposes and Structure of the Fourth Amendment

For better or for worse, we currently regulate law enforcement in the United States with a constitutional regulatory regime, comprised primarily by the Fourth, Fifth, and Sixth Amendments. A significant part of this regime applies to government information-gathering. The Fifth Amendment affords individuals a privilege against being compelled to testify about incriminating information.¹⁹⁰ The focus of this Part is the Fourth Amendment, which regulates the ability of the government to obtain information through searches and seizures. The Fourth Amendment provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath

189. GARROW, *supra* note 117, at 209.

190. See U.S. CONST. amend. V.

or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.¹⁹¹

The Fourth Amendment contains two clauses, the first establishing the right to be secure in persons, houses, papers, and effects against unreasonable searches and seizures and the second stating the requirements for a valid warrant. A long running debate in Fourth Amendment discourse concerns the relationship between the clauses.¹⁹²

Substantively, the Fourth Amendment's focus has been on protecting privacy against certain government activities. Procedurally, permissible exercises of government power are controlled through the process of obtaining a warrant supported by probable cause.

The first and most important issue in Fourth Amendment analysis is whether the Fourth Amendment applies to the particular government action. Although the Fourth Amendment applies to government activity in both the civil and criminal contexts,¹⁹³ it is limited to activities that constitute "searches" and "seizures." Certain activities, such as seeing things in public, are not searches.¹⁹⁴ Further, the Court has held that the Fourth Amendment only governs searches where an individual has a reasonable expectation of privacy.¹⁹⁵

Once the Fourth Amendment applies, a search or seizure must be "reasonable."¹⁹⁶ Although technically the two clauses of the Fourth Amendment are separate, the Court has interpreted the requirement that a search or seizure be reasonable as closely related to the requirement of a warrant. Generally, searches and seizures without a warrant are per se unreasonable.¹⁹⁷ This has become known as the "per se" warrant rule.¹⁹⁸

Even if the requirements for a valid warrant are established, the Fourth Amendment prohibits the search if it is unreasonable.¹⁹⁹ However, the

191. U.S. CONST. amend. IV.

192. See generally AKHIL REED AMAR, *THE CONSTITUTION AND CRIMINAL PROCEDURE* (1997); Silas J. Wasserstrom, *The Fourth Amendment's Two Clauses*, 26 AM. CRIM. L. REV. 1389 (1989).

193. AMAR, *supra* note 192, at 9.

194. See, e.g., *Harris v. United States*, 390 U.S. 234, 236 (1968) ("It has long been settled that objects falling in the plain view of an officer who has a right to be in the position to have that view are subject to seizure and may be introduced in evidence.").

195. See *Katz v. United States*, 389 U.S. 347, 347 (1967). For a discussion of the reasonable expectation of privacy test, see *infra* Part III.A.2.

196. See U.S. CONST. amend. IV.

197. See AMAR, *supra* note 192, at 3-4.

198. See *id.*; Sherry F. Colb, *The Qualitative Dimension of Fourth Amendment "Reasonableness,"* 98 COLUM. L. REV. 1642, 1648 (1998); Wasserstrom & Seidman, *supra* note 110, at 26-27.

199. See AMAR, *supra* note 192, at 16.

Court has rarely found that a search conducted pursuant to a warrant supported by probable cause was unreasonable.²⁰⁰ Unfortunately, as commentators have pointed out, when the Court has approached what is “reasonable,” it has failed to give “reasonable” any teeth.²⁰¹ Therefore, if the government obtains a valid search warrant, in most cases the search or seizure is reasonable so long as it is properly within the scope of the warrant.

To obtain a warrant, the police must demonstrate to a neutral judge or magistrate that they have “probable cause”—“where ‘the facts and circumstances within [the police’s] knowledge and of which they had reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has been or is being committed.’”²⁰²

Despite the Court’s pronouncement in *Katz* in 1967 that there are only “a few specifically established and well-delineated exceptions” to the warrant requirement,²⁰³ in the decades following *Katz*, the Court has made numerous exceptions.²⁰⁴ For example, the Court held in *Terry v. Ohio*²⁰⁵ that the police could stop and frisk an individual without a warrant or probable cause. Further, the Court has held that “special needs” in the contexts of schools and workplaces make the warrant and probable cause requirements impracticable.²⁰⁶ In the words of Silas Wasserstrom and

200. The most famous example is *Winston v. Lee*, 470 U.S. 753 (1985), where the Court held that a surgical incision to remove a bullet from the suspect’s body to provide evidence was unreasonable, warrant notwithstanding. However, the Court has sustained a number of other bodily intrusions to obtain evidence, such as the withdrawal of blood to test for blood alcohol level. See *Schmerber v. California*, 384 U.S. 757, 757 (1966).

201. See, e.g., Colb, *supra* note 198, at 1645, 1687–88 (1998) (pointing out the lack of teeth in the Court’s current Fourth Amendment reasonableness balancing and proposing that the Court “recognize that an ‘unreasonable’ search in violation of the Fourth Amendment occurs whenever the intrusiveness of a search outweighs the gravity of the offense being investigated”); Tracey Maclin, *Constructing Fourth Amendment Principles from the Government Perspective: Whose Amendment Is It, Anyway?*, 25 AM. CRIM. L. REV. 669, 719 (1988).

202. *Brinegar v. United States*, 338 U.S. 160, 175–76 (1949).

203. *Katz v. United States*, 389 U.S. 347, 357 (1967).

204. See AMAR, *supra* note 192, at 3–4; Christopher Slobogin, *The World Without a Fourth Amendment*, 39 UCLA L. REV. 1, 18 (1991).

205. 392 U.S. 1, 1 (1968). See also *Camara v. Municipal Court*, 387 U.S. 523 (1967) (holding that although health, fire, and safety inspectors could not enter a home without a warrant, they need not demonstrate probable cause to obtain the warrant). For a critique of *Terry* and *Camara*, see Scott E. Sundby, *A Return to Fourth Amendment Basics: Undoing the Mischief of Camara and Terry*, 72 MINN. L. REV. 383 (1988).

206. See, e.g., *Vernonia Sch. Dist. v. Acton*, 515 U.S. 646 (1995) (drug testing by school officials); *Nat’l Treasury Employees Union v. Von Rabb*, 489 U.S. 656 (1989) (drug testing of Customs officials); *Skinner v. Ry Labor Executives Ass’n*, 489 U.S. 602 (1989) (drug testing of railroad

Louis Michael Seidman, the per se warrant rule “is so riddled with exceptions, complexities, and contradictions that it has become a trap for the unwary.”²⁰⁷

Currently, the Amendment is enforced primarily through the exclusionary rule²⁰⁸ and, to a lesser degree, through civil liability in § 1983 actions.²⁰⁹ In 1961, in *Mapp v. Ohio*,²¹⁰ the Court held that in all criminal proceedings, both federal and state, evidence obtained in violation of the Fourth Amendment must be excluded from the defendant’s criminal trial.²¹¹ According to Arnold Loewy: “The exclusionary rule protects innocent people by eliminating the incentive to search and seize unreasonably.”²¹² Without the exclusionary rule, Justice Holmes observed, the Fourth Amendment would be a mere “form of words.”²¹³ The exclusionary rule, however, has long been a sore spot in Fourth Amendment jurisprudence, engendering an extensive debate over its desirability and efficacy.²¹⁴

employees); *O’Connor v. Ortega*, 480 U.S. 709 (1987) (search by government employer); *New Jersey v. TLO*, 469 U.S. 325 (1985) (search by school officials).

207. *Wasserstrom & Seidman, supra* note 119, at 34.

208. *See Mapp v. Ohio*, 367 U.S. 643, 657 (1961) (holding that the exclusionary rule applies to all government searches, state and federal).

209. Liability under § 1983 has been severely limited due to qualified immunity for police officers, *see generally* *Harlow v. Fitzgerald*, 457 U.S. 800 (1982), as well as the lack of direct liability for states. *See generally* *Hans v. Louisiana*, 134 U.S. 1 (1890). Municipalities and local governments can be sued, but they are only liable “when execution of a government’s policy or custom, whether made by its lawmakers or by those whose edicts or acts may fairly represent official policy inflicts the injury.” *Monell v. New York City Dep’t of Social Services*, 436 U.S. 658, 658 (1978).

210. 367 U.S. 643, 643 (1961).

211. Prior to *Mapp*, the Court held that the exclusionary rule only applied to evidence improperly obtained by federal officials in federal court. *See Weeks v. United States*, 232 U.S. 383, 398 (1914). In *Wolf v. Colorado*, 338 U.S. 25 (1949), the Court held that the exclusionary rule does not apply to state officials. In *Elkins v. United States*, 364 U.S. 206 (1960), the Court began to reverse course, holding that evidence seized by state police in violation of Fourth Amendment is excluded in federal court. For more background about the development of the exclusionary rule, see Potter Stewart, *The Road to Mapp v. Ohio and Beyond: The Origins, Development and Future of the Exclusionary Rule in Search and Seizure Cases*, 83 COLUM. L. REV. 1365 (1983).

212. Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229, 1266 (1983).

213. *Silverthorne Lumber Co. v. United States*, 251 U.S. 385, 392 (1920).

214. Several commentators have criticized the exclusionary rule, advocating a system of civil damages rather than the exclusion of inculpatory evidence. *See* AMAR, *supra* note 192, at 28 ([the criminal defendant is] an awkward champion of the Fourth Amendment. . . . He is often unrepresentative of the larger class of law-abiding citizens, and his interests regularly conflict with theirs.”); *Id.* at 20–21 (suggesting tort remedies); Christopher Slobogin, *Why Liberals Should Chuck the Exclusionary Rule*, 1999 U. ILL. L. REV. 363, 400–01 (1999) (arguing for a damages remedy because the exclusionary rule fails to provide an adequate remedy to innocent people whose Fourth Amendment rights are violated and because the rule results in judicial reluctance to expand Fourth Amendment protection). Other commentators argue that civil damages will prove to be much less successful than

2. Fourth Amendment Scope: Privacy

As applied by the Court, the Fourth Amendment has focused on protecting against invasions of privacy,²¹⁵ although some commentators contend this focus is misguided. According to William Stuntz, criminal procedure is “firmly anchored in a privacy value that had already proved inconsistent with the modern state.”²¹⁶ For Stuntz, privacy vis-à-vis the government is impracticable given the rise of the administrative state, with its extensive health and welfare regulation. Stuntz asserts that robust Fourth Amendment protection of privacy will prevent the government from regulating industry, uncovering white-collar crime, and inspecting industry facilities. The government must collect information to enforce certain regulations, such as securities laws, and worker safety protections.²¹⁷ “By focusing on privacy,” Stuntz argues, “Fourth Amendment law has largely abandoned the due process cases concern with coercion and violence.”²¹⁸ “The problem,” argues Stuntz, “is not information gathering but [police] violence.”²¹⁹

Scott Sundby offers a different critique of the Fourth Amendment’s focus on privacy. Privacy, although “meant to liberate the [Fourth] Amendment from wooden categorizations . . . [, has] turned out to contain the seeds for the later contraction of Fourth Amendment rights.”²²⁰ “The Fourth Amendment as a privacy-focused doctrine has not fared well with the changing times of an increasingly nonprivate world and a judicial reluctance to expand individual rights.”²²¹ The Fourth Amendment should be redefined as promoting “‘trust’ between the government and the citizenry.”²²² In contrast to totalitarian states, where the government

the exclusionary rule. See Loewy, *supra* note 212, at 1266 (arguing that under a damages regime, if the government really wants to search, it will conduct the illegal search and pay the damages); Maclin, *supra* note, 130 at 62 (contending that juries sympathize with the police in civil suits to enforce the Fourth Amendment and that damages are hard to prove).

215. See William J. Stuntz, *Privacy’s Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1019 (1995).

216. Stuntz, *supra* note 119, at 442.

217. See Stuntz, *supra* note 215, at 1019.

218. Stuntz, *supra* note 119, at 446. See also Stuntz, *supra* note 215, at 1044 (“Coercion becomes the law’s focus only in . . . the most extreme cases. Elsewhere, the law’s chief concern remains privacy”).

219. Stuntz, *supra* note 215, at 1077.

220. Scott E. Sundby, “Everyman”’s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?, 94 COLUM. L. REV. 1751, 1757–58 (1994).

221. *Id.* at 1771.

222. *Id.* at 1777.

demonstrates a profound distrust of the people, the government should “trust that the citizenry will exercise its liberties responsibly.”²²³

However, Sundby assumes that “privacy” means what the Court says it means. Many current problems in Fourth Amendment jurisprudence stem from the Court’s failure to conceptualize privacy adequately, both in method and substance. Methodologically, the Court has attempted to adhere to a unified conception of privacy. Conceptualizing privacy by attempting to isolate its essence or common denominator has inhibited the Court from conceptualizing privacy in a way that can adapt to changing technology and social practices.²²⁴ Consider that, substantively, the Court originally conceptualized privacy in physical terms as protecting tangible property or preventing trespasses²²⁵ and that after *Katz*, the Court shifted to viewing privacy as a form of total secrecy.²²⁶ In each of these conceptual paradigms, the Court has rigidly adhered to a single narrow conception and has lost sight of the Fourth Amendment’s larger purposes.

In contrast, the Fourth Amendment provides for an architecture of power, a structure of protection that safeguards a range of different social practices of which privacy forms an integral dimension. Those like Stuntz and Sundby who contend that the Fourth Amendment should not concern itself with privacy fail to see the importance of privacy in the relationship between the government and the people. The private life is a critical point for the exercise of power. Privacy involves aspects of our lives and social practices where people feel vulnerable, uneasy, and fragile. It involves aspects where the norms of social judgment are particularly abrasive and oppressive. It is also implicated where information relates to issues of our most basic needs and desires: finances, employment, entertainment, political activity, sexuality, and family. The private life is an area of profound sensitivity. Control over the private life is one of the central techniques of government power in totalitarian states. Indeed, the great dystopian novels of the twentieth century—George Orwell’s *Nineteen Eighty-Four*, Aldous Huxley’s *Brave New World*, and Franz Kafka’s *The Trial*, illustrate how government exercises of power over the private life stifle freedom and well-being.²²⁷

223. *Id.*

224. See Solove, *supra* note 17, at 1146–47.

225. See *infra* Part III.A.2.

226. See *infra* Part III.A.2.

227. See ALDOUS HUXLEY, *BRAVE NEW WORLD* (1932); FRANZ KAFKA, *THE TRIAL* (Willa & Edwin Muir, et. al., trans., Alfred A. Knopf, Inc. 1956) (1937); ORWELL, *supra* note 96.

Although Stuntz contends that the Fourth Amendment must turn away from privacy after the rise of the administrative state, this is the very reason why it is so important to protect privacy. The rise of the administrative state threatens to give the government excessive power that could destroy the Framers' careful design to ensure that the power of the People remains the strongest.²²⁸ In particular, the extensive power of modern bureaucracies over individuals depends in significant part on the collection and use of personal information. While Stuntz is correct that the Fourth Amendment should not be cabined exclusively to protecting privacy and should address other values, such as coercion and violence, he errs in treating privacy and police coercion as mutually exclusive.²²⁹

Further, robust Fourth Amendment protection need not be inconsistent with the administrative state, as a significant portion of modern administrative regulation concerns business and commercial activities which lack Fourth Amendment rights equivalent to those guaranteed to individuals.²³⁰ Stuntz retorts that for individuals to have a meaningful protection of privacy, they must have privacy within institutions, and giving privacy rights to individuals within institutions "is almost the same as giving the institution itself a protectible privacy interest."²³¹ Further, Stuntz contends, "a great deal of government information gathering targets individuals," such as the information that is gathered in tax forms.²³² However, one need not adopt an all-or-nothing approach to Fourth Amendment privacy. The Fourth Amendment does not categorically prohibit the government from compelling certain disclosures by individuals or institutions. If it did, then a significant amount of corporate regulation and the tax system would be nearly impossible to carry out. But the fact that the government can compel certain disclosures does not mean that it

228. Raymond Shih-Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1340 (2002) (examining connection between the Fourth Amendment to separation of powers).

229. See Daniel Yeager, *Does Privacy Really Have a Problem in the Law of Criminal Procedure?*, 49 RUTGERS L. REV. 1283, 1309–10 (1997) (agreeing with Stuntz that regulatory inspections can be more invasive of privacy than regular searches, but disagrees that "encounterless police investigations should be more loosely controlled so they are better aligned with regulatory inspections"). Louis Michael Seidman disputes Stuntz's view that the Fourth Amendment places privacy above coercion. See generally Louis Michael Seidman, *The Problems with Privacy's Problem*, 93 MICH. L. REV. 1079 (1995).

230. Although corporations are deemed "persons" under the Fourteenth Amendment, see *Santa Clara County v. S. Pac. R.R.*, 118 U.S. 394, 394–95 (1886), they are not afforded Fourth Amendment rights. See *California Bankers Ass'n v. Shultz*, 416 U.S. 21, 65 (1974) (stating that "corporations can claim no equality with individuals in the enjoyment of a right to privacy").

231. Stuntz, *supra* note 215, at 1037.

232. *Id.*

can compel people to disclose the details of their sexual lives or require them to send in their diaries and personal papers along with their tax forms. Further, the fact that the government can inspect factories for safety violations and food processing facilities for health violations does not mean that the government should be able to search every employee's office, locker, or bag. Therefore, although misconceptualizing privacy, the Court has correctly made it a focal point of the Fourth Amendment.

3. Fourth Amendment Structure: Warrants

Before eroding it with dozens of exceptions, the Court made the Fourth Amendment's warrant requirement one of the central mechanisms to ensure that the government was exercising its powers of information gathering responsibly. Some critics, however, view warrants as relatively unimportant in the Fourth Amendment scheme, as something to be restricted rather than expanded. According to Akhil Amar, the Fourth Amendment "does not require, presuppose, or even prefer warrants—it *limits* them. Unless warrants meet certain strict standards, they are per se unreasonable."²³³ Amar contends that the colonial revolutionaries viewed warrants with disdain because judges were highly influenced by the Crown and warrants immunized government officials from civil liability after conducting a search.²³⁴ Therefore, according to Amar, "[t]he core of the Fourth Amendment, as we have seen, is neither a warrant nor probable cause, but reasonableness."²³⁵

Amar is too dismissive of warrants. Merely looking to colonial precedents is insufficient, because the Fourth Amendment did not follow colonial precedents (since general searches were rampant) but "repudiate[d] them."²³⁶ My aim, however, is not to quarrel about original intent, as it remains unclear whether the per se warrant rule follows the Framers' intent. Even if Amar is right about the Framers' intent, warrants are an important device in our times since, as Scott Sundby observes, "the Founders could not have foreseen the technological and regulatory reach of government intrusions that exists today."²³⁷

The warrant requirement embodies two important insights of the Framers that particularly hold true today. First, the warrant requirement

233. AMAR, *supra* note 192, at 11.

234. *See id.*

235. *Id.* at 31.

236. LEVY, *supra* note 130, at 154.

237. Sundby, *supra* note 220, at 1804.

aims to prevent searches from turning into “fishing expeditions.”²³⁸ Accordingly, the warrant clause circumscribes searches and seizures. A warrant must describe with “particular[ity] . . . the place to be searched and the persons or things to be seized.”²³⁹

The Framers included the warrant clause because of their experience with general warrants and writs of assistance.²⁴⁰ The colonists despised writs of assistance because they authorized “sweeping searches and seizures without any evidentiary basis.”²⁴¹ The Fourth Amendment was inspired by the use of general warrants by Britain, which “resulted in ‘ransacking’ and seizure of the personal papers of political dissenters, authors, and printers of seditious libel.”²⁴² As Patrick Henry declared: “They may, unless the general government be restrained by a bill of rights, or some similar restrictions, go into your cellars and rooms, and search, ransack, and measure, everything you eat, drink, and wear. They ought to be restrained within proper bounds.”²⁴³

Second, warrants reflect James Madison’s vision of the appropriate architecture of power for a society in which the power of the people remains paramount. Writing about separation of powers in *Federalist No. 51*, Madison observed:

But what is government itself but the greatest of all reflections on human nature? If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controuls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: You must first enable the government to controul the governed; and in the next place, oblige it to controul itself. A dependence on the people is no doubt the primary controul on the government; but experience has taught mankind the necessity of auxiliary precautions.²⁴⁴

238. Louis Fisher, *Congress and the Fourth Amendment*, 21 GA. L. REV. 107, 115 (1986) (“The spirit and letter of the fourth amendment counseled against the belief that Congress intended to authorize a ‘fishing expedition’ into private papers on the possibility that they might disclose a crime.”).

239. U.S. CONST. amend. IV.

240. Maclin, *supra* note 130, at 8. Indeed, as Maclin notes: “Everyone, including Amar, agrees that the Framers opposed general warrants.” *Id.* at 9. See also LEVY, *supra* note 130, at 158.

241. Wasserstrom & Seidman, *supra* note 119, at 82.

242. DAVID M. O’BRIEN, *PRIVACY, LAW, AND PUBLIC POLICY* 38 (Prager Publishers 1979). See also LEVY, *supra* note 130, at 150; Stuntz, *supra* note 119, at 406.

243. 3 THE DEBATES IN SEVERAL CONVENTIONS ON THE ADOPTION OF THE FEDERAL CONSTITUTION 448–49 (Jonathan Elliot ed., 1974).

244. James Madison, *The Federalist, No. 51*, in THE FEDERALIST 347, 349 (Jacob E. Cooke ed., 1961).

The profound insight of Madison and the Framers was that by separating government powers between different entities and pitting them against each other, government could be controlled. Madison was acutely aware that the “parchment barriers” of the Constitution would fail to check government encroachments of power, and he explained how both the legislative and executive branches could overstep their bounds.²⁴⁵ He therefore reasoned that government power should be constrained through governmental architecture, not mere restrictive words.²⁴⁶ As Madison put it, power should be diffused among different departments of government, each of which should be given “the necessary constitutional means, and personal motives, to resist encroachments of the others,”²⁴⁷ because government will be kept in check only if its parts consist of “opposite and rival interests.”²⁴⁸ Gordon Wood aptly described the Madisonian vision:

It was an imposing conception—a kinetic theory of politics—such a crumbling of political and social interests, such an atomization of authority, such a parceling of power, not only in the governmental institutions but in the extended sphere of the society itself, creating such a multiplicity and a scattering of designs and passions, so many checks, that no combination of parts could hold, no group of evil interests could long cohere. Yet out of the clashing and checking of this diversity, Madison believed the public good, the true perfection of the whole, would somehow arise.²⁴⁹

The warrant requirement reflects Madison’s philosophy of government power by inserting the judicial branch in the middle of the executive branch’s investigation process.²⁵⁰ Although warrants have been criticized as ineffective because judges and magistrates often defer to the police and prosecutor’s determination, Christopher Slobogin aptly contends that warrants raise the “standard of care” of law enforcement officials by forcing them to “document their requests for authorization.”²⁵¹ According to Stuntz, warrants make searching more expensive, because they require law enforcement officials to “draft affidavits and wait around

245. James Madison, *The Federalist*, No. 48, *supra* note 244, at 333 (James Madison).

246. Madison, *supra* note 244, at 347 (James Madison).

247. *Id.* at 349.

248. *Id.*

249. GORDON S. WOOD, *THE CREATION OF THE AMERICAN REPUBLIC 1776–1787* 605 (Univ. of North Carolina Press 1969).

250. Madison drafted the language of the Fourth Amendment. See Fisher, *supra* note 238, at 111–12. As Levy observes, “Madison chose the maximum protection conceivable at the time.” LEVY, *supra* note 130, at 176.

251. Slobogin, *supra* note 204, at 17.

courthouses.”²⁵² Because officers must devote time to obtaining a warrant, they are unlikely to use them unless they think it is likely that they will find what they are looking for.²⁵³ As Justice Douglas has explained for the Court:

We are not dealing with formalities. The presence of a search warrant serves a high function. Absent some grave emergency, the Fourth Amendment has interposed a magistrate between the citizen and the police. This was done neither to shield criminals nor to make the home a safe haven for illegal activities. It was done so that an objective mind might weigh the need to invade that privacy in order to enforce the law. The right of privacy was deemed too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of criminals. Power is a heady thing; and history shows that the police acting on their own cannot be trusted. And so the Constitution requires a magistrate to pass on the desires of the police before they violate the privacy of the home.²⁵⁴

Further, the requirement of prior approval prevents government officials from “dreaming up post hoc rationalizations”²⁵⁵ and from experiencing judicial hindsight bias when evaluating the propriety of a search after it has taken place.²⁵⁶ As Raymond Ku aptly observes, the Framers adopted the Fourth Amendment based on concerns about limiting executive power.²⁵⁷

My purpose is not to defend the existing structure of the Fourth Amendment as perfect. For the purposes of this Article, it is sufficient to agree (1) that the Fourth Amendment regime serves an important function by establishing an architecture of power that aims to protect privacy in addition to other values, and (2) that one of the central features of this architecture requires neutral and external oversight of the executive branch’s power to gather and use personal information.

252. William J. Stuntz, *O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842, 848 (2001).

253. *See id.* at 848.

254. *McDonald v. United States*, 335 U.S. 451, 455–56 (1948). *See also Steagald v. United States*, 451 U.S. 204, 212 (1981) (warrants are necessary because law enforcement officials “may lack sufficient objectivity”); *Coolidge v. New Hampshire*, 403 U.S. 443, 450 (1971) (stating that “prosecutors and policemen simply cannot be asked to maintain the requisite neutrality with regard to their own investigations”); *Johnson v. United States*, 333 U.S. 10, 13–14 (1948) (stating that the Fourth Amendment ensures that inferences of potential culpability “be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime”).

255. AMAR, *supra* note 192, at 39.

256. *See Steiker*, *supra* note 121, at 853.

257. Ku, *The Founders’ Privacy*, *supra* note 228, at 1333–40.

Even if its efficacy is limited, the structure of the Fourth Amendment is better than a void. Few commentators have suggested that the Fourth Amendment be repealed or that its larger purposes in controlling government power are inimical to a well-functioning society. Outside the realm of the Fourth Amendment is a great wilderness, a jungle of government discretion and uncontrolled power. Thus, the issue of the applicability of the Fourth Amendment is an important one, and to that issue I now turn.

B. THE SHIFTING PARADIGMS OF FOURTH AMENDMENT PRIVACY

Some notion of privacy was always the trigger for Fourth Amendment protection, at least since the late nineteenth century. In 1886, in *Boyd v. United States*,²⁵⁸ an early case delineating the meaning of the Fourth and Fifth Amendments,²⁵⁹ the government attempted to subpoena the records of a merchant for use in a civil forfeiture proceeding.²⁶⁰ The Court held that the subpoena violated the Fourth and Fifth Amendments:

It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property, where that right has never been forfeited by his conviction of some public offence²⁶¹

Commentators have characterized *Boyd* as protecting property and as consistent with the exaltation of property and contract during the *Lochner*-era.²⁶² Although *Boyd* certainly furthers the ideology of the *Lochner* Court, it should not merely be dismissed as the product of *Lochner*-like activism. *Boyd* follows a conception of privacy that the Court consistently adhered to in the late nineteenth century and the first half of the twentieth century. Under this conception, the Court views invasions of privacy as a type of physical injury involving incursions into tangible things.

258. 116 U.S. 616 (1886).

259. The Fifth Amendment provides that: "No person . . . shall be compelled in any criminal case to be a witness against himself . . ." U.S. CONST. amend. V. The Fifth Amendment's "privilege against self-incrimination" prevents the government from compelling individuals to disclose inculpatory information about themselves. *Id.*

260. See *Boyd*, 116 U.S. at 617–18.

261. *Id.* at 630.

262. See, e.g., AMAR, *supra* note 192, at 22 (explaining that *Boyd* was part of the *Lochner* Court's staunch protection of property); O'BRIEN, *supra* note 242, at 22 (explaining that *Boyd* associated privacy with "proprietary interests"); ALAN WESTIN, *PRIVACY AND FREEDOM* 339–41 (1967) (describing the conception of privacy in *Boyd* as "propertied privacy"); Stuntz, *supra* note 215, at 1030–34 (describing *Boyd* as part of *Lochner* Court's impediment to the rise of the administrative state).

The protection of tangible things extended beyond the home, encompassing the opening of letters sent via the postal system. Nine years prior to *Boyd*, the Court recognized in 1877, in *Ex Parte Jackson*,²⁶³ that “[t]he constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be.”²⁶⁴ Additionally, privacy also concerned physical bodily intrusions. In *Union Pacific Railway Company v. Botsford*,²⁶⁵ an 1891 case concerning privacy but not directly involving the Fourth Amendment, the Court held that a court could not compel a female plaintiff in a civil action to submit to a surgical examination:

The inviolability of the person is as much invaded by a compulsory stripping and exposure as by a blow. To compel any one, and especially a woman, to lay bare the body, or to submit it to the touch of a stranger, without lawful authority, is an indignity, an assault, and a trespass²⁶⁶

Consistent with *Boyd* and *Ex Parte Jackson*, the Court readily recognized the injury caused by physical intrusions such as trespassing into homes, rummaging through one’s things, seizing one’s papers, opening and examining one’s letters, or physically touching one’s body. Indeed, in 1890, when Warren and Brandeis authored their famous article *The Right to Privacy*, they observed that the law, which had long recognized physical and tangible injuries, was just beginning to recognize incorporeal ones.²⁶⁷ Warren and Brandeis argued that privacy was more than simply a physical intrusion,²⁶⁸ a view increasingly recognized in the common law of torts in the early twentieth century.²⁶⁹ However, in its Fourth Amendment jurisprudence, the Court held fast to its physical intrusion conception of privacy.

The Court’s view that Fourth Amendment privacy constituted protection from physical intrusions came to a head in 1928 in *Olmstead v. United States*.²⁷⁰ There, the Court held that the tapping of a person’s home

263. 96 U.S. 727 (1877).

264. *Id.* at 733.

265. 141 U.S. 250 (1891).

266. *Id.* at 252.

267. See Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193–95 (1890).

268. See *id.* at 195–97.

269. See Irwin R. Kramer, *The Birth of Privacy Law: A Century Since Warren and Brandeis*, 39 CATH. U. L. REV. 703, 704 (1990).

270. 277 U.S. 438 (1928).

telephone outside a person's house did not run afoul of the Fourth Amendment because it did not involve a trespass inside a person's home. More specifically, it held that "[t]he Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants."²⁷¹ *Olmstead* relied upon the Court's physical intrusion conception of privacy. Since there was no trespassing, opening, or rummaging, there was no invasion of Fourth Amendment privacy.

Justice Louis Brandeis vigorously dissented, chastising the Court for failing to adapt the Constitution to new problems. He observed: "When the Fourth and Fifth Amendments were adopted, the form that evil had theretofore taken had been necessarily simple."²⁷² Furthermore, "[the government] could secure possession of [a person's] papers and other articles incident to his private life—a seizure effected, if need be, by breaking and entry."²⁷³ Brandeis argued that the Fourth Amendment was designed to regulate this conduct—that

'time works changes, brings into existence new conditions and purposes.' Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.²⁷⁴

The Court, however, followed the *Olmstead* conception of privacy in *Goldman v. United States*.²⁷⁵ The police placed a device called a "detectaphone" on the wall next to a person's office enabling them to eavesdrop on the conversations inside the office.²⁷⁶ The Court concluded that since there had been no physical trespass into the office, the Fourth Amendment had not been violated.²⁷⁷

In 1967, nearly forty years after *Olmstead*, the Court in *Katz v. United States*²⁷⁸ finally abandoned the physical intrusion conception of privacy, and adopted the Fourth Amendment approach employed today. *Katz* involved the wiretapping of a telephone conversation made by the

271. *Id.* at 464.

272. *Id.* at 473 (Brandeis, J., dissenting) (internal quotations omitted).

273. *Id.*

274. *Id.* at 473.

275. 316 U.S. 129 (1942).

276. *Id.*

277. *See id.* at 134.

278. 389 U.S. 347 (1967).

defendant while in a phone booth. Explicitly overruling *Olmstead* and *Goldman*, the Court declared: “What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”²⁷⁹

The Court’s approach to determining the applicability of the Fourth Amendment emerged from Justice Harlan’s concurrence in *Katz*. The “reasonable expectation of privacy test” looks to whether (1) a person exhibits an “actual or subjective expectation of privacy” and (2) “the expectation [is] one that society is prepared to recognize as ‘reasonable.’”²⁸⁰

Brandeis’ dissent in *Olmstead* only partially won the day in *Katz*. Instead of adopting a conception of privacy that was adaptable to technology, as the new reasonable expectation of privacy test initially had promised to be, the Court rigidified its approach with a particular conception of privacy—total secrecy. The Court centered this new conception on the language in *Katz*, indicating that privacy turned on what a person exposed to the public. In this way, privacy was conceptualized as a form of secrecy, and one could not have a reasonable expectation of privacy in information that was not kept secret.

The full implications of this new conception of privacy are discussed in the next section. Before turning to this issue, it is important to observe the effects of the Court’s failure to conceptualize privacy in *Olmstead*. As a result of the nearly forty years between *Olmstead* and *Katz*, there has been little control over the burgeoning use of electronic surveillance. Electronic surveillance, one of the most powerful technological law enforcement tools developed during the twentieth century, has profoundly increased the government’s powers. The Fourth Amendment, however, has stood by silently as this new technology has developed.

At the time of *Olmstead*, many viewed wiretapping with great unease. Justice Holmes called it a “dirty business.”²⁸¹ Even those who became its greatest abusers had initially criticized it. J. Edgar Hoover testified in 1929 that “while it may not be illegal . . . [wiretapping] is unethical and it is not

279. *Id.* at 351–52.

280. *Id.* at 361 (Harlan, J., concurring).

281. *Olmstead*, 277 U.S. 438, 470 (1928) (Holmes, J., dissenting). See also RICHARD F. HIXSON, *PRIVACY IN A PUBLIC SOCIETY: HUMAN RIGHTS IN CONFLICT* 49 (1987). For a history of the early days of wiretapping, see Note, *The Right to Privacy in Nineteenth Century America*, 94 HARV. L. REV. 1892 (1981).

permitted under the regulations by the Attorney General.”²⁸² Hoover stated that “any employee engaged in wire tapping will be dismissed from the service of the bureau.”²⁸³

In 1934, just six years after *Olmstead*, Congress enacted § 605 of the Federal Communications Act, making wiretapping a federal crime. However, § 605 had significant limitations. It did not apply to wiretapping by state law enforcement officials or by private parties. Nor did it apply to bugging. Further, federal law enforcement officials interpreted § 605 merely to preclude the disclosure rather than the collection of intercepted communications.²⁸⁴ The Supreme Court, however, held that § 605 precluded evidence obtained by wiretapping from being used in court.²⁸⁵ Although law enforcement officials could not use wiretapping evidence or its fruits, § 605 failed to prevent them from installing devices and listening.²⁸⁶

Gradually, presidents gave the FBI increasing authority to wiretap.²⁸⁷ In World War II, the FBI was authorized to engage in wiretapping to investigate threats to national security. Later, the authorization for wiretapping expanded to encompass domestic security. The fear of communism during the 1950s resulted in further increases in the use of electronic surveillance.²⁸⁸

As fears of Communism escalated and the authority to engage in electronic surveillance increased, widespread abuses began to occur. Hoover substantially abused his wiretapping authority by extensively wiretapping FBI critics, individuals whose views he disliked, and the enemies of his political allies.²⁸⁹ As discussed earlier, he engaged in massive electronic surveillance of Martin Luther King, Jr.²⁹⁰ Presidents also used the wiretapping power of the FBI for their own political purposes and for domestic surveillance. President Nixon ordered extensive wiretapping, including surveillance of his own speechwriter, William

282. Fisher, *supra* note 238, at 127.

283. *Id.*

284. ROBERT ELLIS SMITH, BEN FRANKLIN’S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 158 (2000).

285. See *Nardone v. United States*, 302 U.S. 379 (1937) (evidence directly obtained by wiretapping excluded from evidence); *Nardone v. United States*, 308 U.S. 338 (1939) (evidence obtained as the fruit of illegal wiretapping could not be used in court).

286. See SMITH, *supra* note 284, at 160.

287. See DIFFIE & LANDAU, *supra* note 128, at 155–65.

288. See DIFFIE & LANDAU, *supra* note 128, at 161–62.

289. See *supra* Part II.C.

290. See *supra* Part II.C.

Safire.²⁹¹ Presidents Kennedy and Johnson have also been accused of ordering electronic surveillances for improper purposes.²⁹² With regard to pre-*Katz* wiretapping by the states, an influential study led by Samuel Dash concluded that 90% of state wiretapping had been done without court authorization and that state regulation of wiretapping had been largely ineffective and impotent against abuses.²⁹³

Thus, for forty years, the government's power to engage in electronic surveillance has fallen outside of the reach of the Fourth Amendment, and the legislation that has filled the void has been ineffective. Today, history is in the process of repeating itself. The Court has made a mistake similar to the one the *Olmstead* Court made, and it is one with severe and far-reaching implications.

C. THE NEW *OLMSTEAD*

Although we have moved from the *Boyd* and *Olmstead* world of physical papers and places to a new regime based upon expectations of privacy, there is a new *Olmstead*, one that is just as shortsighted and rigid in approach. The Court's new conception of privacy is one of total secrecy. If any information is exposed to the public or if law enforcement officials can view something from any public vantage point, then the Court has refused to recognize a reasonable expectation of privacy.

For example, in *Florida v. Riley*,²⁹⁴ the Court held that a person did not have a reasonable expectation of privacy in his enclosed greenhouse because a few roof panels were missing and the police were able to fly over it with a helicopter.²⁹⁵ In *California v. Greenwood*,²⁹⁶ the police searched plastic garbage bags that the defendant had left on the curb to be collected by the trash collector. The Court held that there was no reasonable expectation of privacy in the trash because "[i]t is common knowledge that plastic bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public."²⁹⁷ The Court also reasoned that the trash was left at the curb "for the express purpose of conveying it to a third party, the trash collector, who might

291. See *DIFFIE & LANDAU*, *supra* note 128, at 144.

292. *Id.* at 173.

293. SAMUEL DASH, RICHARD SCHWARTZ, & ROBERT KNOWLTON, *THE EAVESDROPPERS* (1959).

294. 488 U.S. 445 (1989).

295. See *id.* at 451–52.

296. 486 U.S. 35 (1988).

297. *Id.* at 40.

himself have sorted through [the] trash or permitted others, such as the police, to do so.”²⁹⁸

Consistent with this conception of privacy, the Court held that there is no reasonable expectation in privacy for information known or exposed to third parties. In *United States v. Miller*,²⁹⁹ federal agents presented subpoenas to two banks to produce all of the financial records of the defendant. The banks produced the records but did not notify the defendant of the subpoenas. The defendant challenged the subpoenas as a violation of the Fourth Amendment. The Court held that there was no reasonable expectation of privacy in financial records maintained by a bank.³⁰⁰ “[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities.”³⁰¹ The Court reasoned: “The checks are not confidential communications but negotiable instruments to be used in commercial transactions. All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.”³⁰²

In *Smith v. Maryland*, police officers were attempting to track down a robber who had begun making obscene and harassing phone calls.³⁰³ At one point, the robber asked someone he had been calling to step out on her front porch, where she observed him drive by in his car.³⁰⁴ The police traced the license plate number and found that the car was registered to the defendant.³⁰⁵ Without a warrant, the police asked the telephone company to install a pen register to record the numbers dialed from the defendant’s home.³⁰⁶ The Court concluded that there was no reasonable expectation of privacy in pen registers.³⁰⁷ Since people “know that they must convey numerical information to the phone company” and that the phone company records this information for billing purposes, people cannot “harbor any general expectation that the numbers they dial will remain secret.”³⁰⁸

298. *Id.*

299. 425 U.S. 435, 435 (1976).

300. *Id.* at 444.

301. *Id.* at 443.

302. *Id.* at 442.

303. 442 U.S. 735, 737 (1979).

304. *Id.*

305. *Id.*

306. *Id.* A pen register is a device that is typically installed at the telephone company’s offices that can record the telephone numbers a person dials. A trap and trace device is a similar device that can record the telephone numbers of a person’s incoming telephone traffic.

307. *Id.* at 743.

308. *Id.*

Miller and *Smith* establish a general rule that if information is in the hands of third parties, then an individual can have no reasonable expectation of privacy in that information, which means that the Fourth Amendment does not apply.³⁰⁹ Individuals thus probably do not have a reasonable expectation of privacy in communications and records maintained by ISPs or computer network system administrators.³¹⁰

Two lines of cases support the third party doctrine. The first deals with standing and the second deals with assumption of risk. The Court's modern standing doctrine emerges primarily from two cases, *Rakas v. Illinois*³¹¹ and *Rawlings v. Kentucky*.³¹²

In *Rakas*, the police seized evidence from the glove compartment of an automobile with several passengers. The passengers moved to suppress the seized evidence under the Fourth Amendment, but the Court held that they had no standing to do so because they did not own the car and because they claimed that they did not own the evidence in the glove compartment. Said the Court, "[a] person who is aggrieved by an illegal search and seizure only through the introduction of damaging evidence secured by a search of a third person's premises or property has not had any of his Fourth Amendment rights infringed."³¹³

In *Rawlings*, a police officer ordered the defendant's girlfriend to empty the contents of her purse. Among the contents of the purse were drugs that the defendant admitted belonged to him. The Court rejected the defendant's Fourth Amendment challenge because he had no reasonable expectation of privacy once he entrusted the items to a third party.³¹⁴

In addition to the standing doctrine, both *Miller* and *Smith* analogized to a series of cases involving the assumption of risk doctrine. In *Miller*, the Court noted that "the Fourth Amendment does not "prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."³¹⁵ In *Smith*, the

309. See ORIN S. KERR, U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS § I.B.3 (Jan. 2001).

310. *Id.* at § I.C.1(b)(iv).

311. 439 U.S. 128 (1978).

312. 448 U.S. 98 (1980).

313. *Rakas*, 439 U.S. at 134.

314. *Rawlings*, 448 U.S. at 104–06.

315. *Miller*, 425 U.S. at 443.

Court stated that the defendant had “assumed the risk that the [phone] company would reveal to the police the numbers he [had] dialed.”³¹⁶

The assumption of risk doctrine emerged from a series of cases dealing with informants and undercover agents. In these cases, either a person had revealed information to a friend, who later divulged the information to the police, or a person revealed the information to a police informant or undercover officer.³¹⁷ For example, in *Hoffa v. United States*,³¹⁸ the Court held that the Fourth Amendment did not apply where the defendant made statements to an undercover informant while in his hotel room.³¹⁹ The Court reasoned that the undercover informant was “not a surreptitious eavesdropper” but was invited in and trusted by the defendant, who had relied “upon his misplaced confidence that [the informant] would not reveal his wrongdoing.”³²⁰ In *Lewis v. United States*,³²¹ the defendant sold drugs to an undercover agent, and the Court held that he had assumed the risk of betrayal.³²² Likewise, in *Lee v. United States*,³²³ the Court relied upon the assumption of risk doctrine to reject the claim of a defendant who had revealed information to an informant who was using a concealed transmitter that enabled the police to listen to the conversation.³²⁴

The third party record doctrine, buttressed by the standing and assumption of risk doctrines, stems from a particular conception of privacy that views Fourth Amendment privacy as constituting a form of total secrecy.³²⁵ Under this conception, privacy is a form of concealment, where secrets are inaccessible to others. If information is not secret in this way, if it is in any way exposed to others, then it loses its status as private.

Further, the Court views privacy as an individual right. Fourth Amendment privacy is enforced at the behest of particular individuals via the exclusionary rule. The problem with the Court’s current conception of privacy is that it views the Fourth Amendment as protecting rights

316. *Smith v. Maryland*, 442 U.S. 735, 744 (1979).

317. *See, e.g., United States v. White*, 401 U.S. 745, 750 (1971) (reasoning that the Fourth Amendment does not protect information conveyed to a government informant who wears a radio transmitter); *On Lee v. United States*, 343 U.S. 747, 754 (1952) (stating that the Fourth Amendment does not apply when a person misplaces her trust by talking to a bugged government informant).

318. 385 U.S. 293 (1966).

319. *Id.* at 302.

320. *Id.*

321. 385 U.S. 206 (1966).

322. *Id.* at 210–11.

323. 343 U.S. at 747.

324. *Id.* at 751–52.

325. *See Solove, supra* note 7, at 1435.

possessed by individuals seeking to suppress evidence. According to Mary Coombs, the Court's Fourth Amendment jurisprudence has applied too much of an "individualistic conception of privacy" and has ignored privacy as shared among groups of individuals.³²⁶ Since the Fourth Amendment establishes an architecture of power, its protection should not turn on whether an individual possesses the right. Rather the Amendment protects rights by establishing a particular social structure, one that benefits society by restricting government power. If we most want to protect innocent parties, the Court's standing doctrine thwarts this very goal.³²⁷

Dissenting in *Rakas*, Justices White, Brennan, Marshall, and Stevens observed that the Court's ruling "undercuts the force of the exclusionary rule in the one area in which its use is most certainly justified—the deterrence of bad-faith violations of the Fourth Amendment."³²⁸ In particular, the Justices observed:

This decision invites police to engage in patently unreasonable searches every time an automobile contains more than one occupant. Should something be found, only the owner of the vehicle, or of the item, will have standing to seek suppression, and the evidence will presumably be usable against the other occupants.³²⁹

Smith and *Miller* have been extensively criticized throughout the past several decades. However, it is only recently that we are truly beginning to see the profound implications of the Court's third party doctrine. *Smith* and *Miller* are the new *Olmstead* and *Goldman*. Gathering information from third party records is an emerging law enforcement practice with as many potential dangers as the wiretapping in *Olmstead*. "The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping," Justice Brandeis observed in his *Olmstead* dissent.³³⁰ "Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by

326. Mary I. Coombs, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 CAL. L. REV. 1593, 1594 (1987). See also Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 367 (1974) (critiquing standing doctrine for viewing Fourth Amendment protections as protecting "atomistic spheres of interest of individual citizens" rather than as "regulation of governmental conduct").

327. See, e.g., Coombs, *supra* note 326, at 1600 (stating that if the purpose of the exclusionary rule is deterrence, then it should apply regardless of standing); Wasserstrom & Seidman, *supra* note 119, at 97 (same).

328. *Rakas v. Illinois*, 439 U.S. 128, 168 (1978) (White, J., dissenting).

329. *Id.* at 168–69.

330. *Olmstead*, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

which it will be enabled to expose to a jury the most intimate occurrences of the home.”³³¹

That day is here. Government information gathering from the extensive dossiers being assembled with modern computer technology poses one of the most significant threats to privacy of our times. In the void left by the inapplicability of the Fourth Amendment, Congress has erected a statutory regime of protection, which establishes the current architecture of power for government information gathering from third party records. Unfortunately, this regime is woefully inadequate.

IV. THE NEW ARCHITECTURE OF POWER: THE EMERGING STATUTORY REGIME AND ITS LIMITS

Throughout the twentieth century, when the Supreme Court held that the Fourth Amendment was inapplicable to new practices or technology, Congress often responded by passing statutes affording some level of protection. Congress through a series of statutes has established a statutory regime regulating government access to third party records. This regime erects a particular architecture of power significantly different from that of the Fourth Amendment. These differences are both substantive (the types of records and information protected) and procedural (the means by which government officials can obtain records). The architecture of this regime is certainly preferable to a void, but is nevertheless substantially inferior to that of the Fourth Amendment. In this Part, I undertake an analysis of this regime, for it is the governing architecture of power for government information-collection from the private sector. Unless the Court reverses course in its Fourth Amendment jurisprudence, it is this regime that must shoulder the burden of balancing order with liberty and keeping government power under control.

A. STATUTORY REGIME ARCHITECTURE: SCOPE

1. Wiretapping and Bugging

When the Court held in *Olmstead* that the Fourth Amendment did not apply to wiretapping, Congress responded six years later by enacting § 605 of the Federal Communications Act of 1934.³³² Pursuant to § 605, “no person not being authorized by the sender shall intercept any

331. *Id.*

332. Former 7 U.S.C. § 605.

communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communications to any person.”³³³ Section 605 did not specify how it was to be enforced, but in *Nardone v. United States*, the Court held that the exclusionary rule applied in federal court to evidence obtained by wiretapping in violation of § 605.³³⁴ However, § 605 was a narrow law that did not apply to the states. Consequently, wiretapping by state law enforcement officials was regulated at the state level, and as an influential report concluded, state wiretapping regulation was relatively ineffective.³³⁵ Further, § 605 did not cover other means of electronic surveillance such as bugging. Finally, the Department of Justice and the FBI interpreted § 605 as only preventing the “divulgence” of information obtained by wiretapping in court, while not prohibiting wiretapping if the information was not used at trial.³³⁶

Section 605 governed wiretapping until *United States v. Katz*, when the Court finally declared that the Fourth Amendment covered wiretapping. In 1968, Congress enacted the Omnibus Crime Control and Safe Streets Act.³³⁷ Title III of the Act substantially improved the law of wiretapping, extending its reach to state officials as well as to private parties.³³⁸

In 1986, Congress amended Title III with the Electronic Communications Privacy Act (ECPA). The ECPA restructured Title III into three titles: Title I (known as the “Wiretap Act”), dealing with the interception of communications;³³⁹ Title II (known as the “Stored Communications Act”), covering access to stored communications and records;³⁴⁰ and Title III (known as the “Pen Register Act”), dealing with pen registers and trap and trace devices.³⁴¹

Three types of communications are covered by the ECPA. A “wire communication” consists of all “aural” transmissions that travel through a wire, cable, or similar medium.³⁴² “Aural” means that the transmission must contain a human voice at some point.³⁴³ An “oral communication,” is

333. *Id.*

334. 302 U.S. 379 (1937).

335. See generally DASH, SCHWARTZ, & KNOWLTON, *supra* note 293.

336. WAYNE R. LAFAVE, JEROLD H. ISRAEL, & NANCY J. KING, CRIMINAL PROCEDURE 260 (3d ed. 2000).

337. Omnibus Crime and Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510–22 (2001).

338. See REGAN, *supra* note 141, at 122–25.

339. Wiretap Act, Electronic Communications Privacy Act, Title I, 18 U.S.C. §§ 2510–22 (2001).

340. Stored Communications Act, Electronic Communications Privacy Act, Title II, 18 U.S.C. §§ 2701–11 (2000).

341. Pen Register Act, Title III, 18 U.S.C. §§ 3121–27 (2000).

342. 18 U.S.C. § 2510(1) (2000).

343. 18 U.S.C. § 2510(18).

one that is “uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation.”³⁴⁴ Typically, oral communications are those intercepted through bugging devices.³⁴⁵ Finally, the third type of communication defined by the ECPA is an “electronic communication.” Electronic communications are all nonwire and nonoral communications that can be transferred through a wide variety of mechanisms.³⁴⁶ Typically these consist of text and images (not the human voice)—an e-mail for instance.³⁴⁷

Title I applies to wiretapping and bugging. A communication must be intercepted in “flight,” during transmission. Title I thus somewhat overlaps with the Fourth Amendment because under *Katz*, the Fourth Amendment applies to wiretapping. Title I further contains an exclusionary rule, making any unlawfully acquired evidence inadmissible.³⁴⁸ However, in a significant limitation, the exclusionary rule does not apply to electronic communications.³⁴⁹ Therefore, the interception of an e-mail is not protected by the exclusionary rule.³⁵⁰

Title I has strict requirements for obtaining a court order in order to engage in electronic surveillance.³⁵¹ In certain respects, Title I’s requirements are stricter than those for a Fourth Amendment search warrant. For instance, Title I restricts the type of officials who may apply for a court order and requires that the officials demonstrate that other means for obtaining the information have been unsuccessful.³⁵² A Title I court order requires probable cause and a specific description of where the communication will be intercepted, the type of communication, and the period of time for the interception.³⁵³ Further, Title I limits the types of crimes that can be investigated with electronic surveillance. For example, a court order cannot be obtained to investigate a misdemeanor. Title I also requires that the court order mandate that the interception be conducted in a

344. 18 U.S.C. § 2510(2).

345. *Id.* § 2510(4).

346. *Id.* § 2510(12).

347. *See id.*

348. *Id.* § 2518 (10)(a) (2000).

349. *See id.*

350. *See id.*

351. *Id.* § 2518.

352. *Id.*

353. *Id.*

way so as to “minimize the interception of communications not subject to interception.”³⁵⁴

With the exception of electronic communications, which are not protected by an exclusionary rule, Title I has substantial protections. However, they cover ground already safeguarded by the Fourth Amendment. As will be illustrated below, the architecture of the statutory regime is much weaker and more porous in the areas not protected by the Fourth Amendment.

2. Stored Communications

Communications service providers frequently store their customers’ communications. These probably fall under the third party-record rule of *Smith v. Maryland*³⁵⁵ and *United States v. Miller*³⁵⁶ because third parties maintain the information.³⁵⁷

Although the Fourth Amendment may not protect stored communications, Title II of the ECPA provides some protection. Title II governs stored communications, such as those stored by a phone company or ISP.³⁵⁸ ISPs temporarily store e-mail communications. For example, suppose Doe sends an e-mail to Roe. The e-mail travels to Roe’s ISP and sits there until Roe logs on and downloads her e-mail. Under certain circumstances, a copy of that e-mail may even be kept by Roe’s ISP after it is downloaded. With many ISPs, users can also keep copies of previously read e-mail on the ISP’s server. Maintaining copies of previously read e-mail with an ISP can be particularly useful, since this enables a person to access the e-mails from remote locations via the Internet. Conversely, if a copy of an e-mail is not kept on the ISP’s computer, then it can be accessed only from the particular computer to which it was downloaded. Additionally, ISPs often maintain an outbox folder that contains copies of all the e-mail that a person has sent out.

Title II restricts the government’s ability to access communications stored by Roe’s ISP.³⁵⁹ Unfortunately, Title II is quite confusing and its protection is limited. Electronic storage is defined as “any *temporary*,

354. 18 U.S.C. § 2518(5).

355. 442 U.S. 735, 735 (1979).

356. 425 U.S. 435, 435 (1976).

357. This conclusion is debatable, however, because telephone companies can also store telephone communications, and it is unlikely that the Court would go so far as to say that this fact eliminates any reasonable expectation of privacy in such communications.

358. 18 U.S.C. §§ 2701–71.

359. *Id.* § 2701.

intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof,” and “any storage of such communication by an electronic communication service for purposes of backup protection.”³⁶⁰ This definition clearly covers e-mail that is waiting on the ISP’s server to be downloaded. However, what about e-mail that has been downloaded by the recipient but maintained by the user on the ISP’s server? According to the Department of Justice’s interpretation of Title II, the copy of the e-mail stored on the server is no longer in temporary storage, and is therefore “simply a remotely stored file.”³⁶¹ Title II permits law enforcement officials to obtain copies of these communications merely by issuing a subpoena to the ISP.³⁶²

Therefore, the process required for government officials to obtain access to stored communications is considerably less stringent than the Fourth Amendment’s warrant requirement. Under Title II, the government must only secure a warrant to obtain the contents of communications in electronic storage for 180 days or less.³⁶³ In the DOJ’s view, these communications encompass only unopened e-mail and not previously accessed e-mail stored on an ISP’s server. For communications stored over 180 days, the government need only obtain an administrative, grand jury or trial subpoena, or a court order.³⁶⁴ No probable cause is required. The government must only offer “specific and articulable facts showing that there are reasonable grounds” to believe communications are “relevant” to the criminal investigation.³⁶⁵ Recall that Title II does not have an exclusionary rule.

3. Records of Communications Providers

Title II also governs a communications service provider’s disclosure of customer records to the government. These provisions differ from the parts of Title II that govern stored communications. Stored communications consist of the traffic of one’s correspondence with others, while customer records consist of information about the customer including

360. 18 U.S.C. § 2510(17) (emphasis added).

361. KERR, *supra* note 309, § III.B.

362. *Id.* at § III.D.1. The government must provide prior or delayed notice to the individual. *See* 18 U.S.C. § 2703(b)(1)(B)(i) & (b)(2).

363. 18 U.S.C. § 2703(a).

364. *Id.* § 2703(b).

365. *Id.* § 2703(d). If the government does not want to provide prior notice to the subscriber that it is seeking the information, it must obtain a warrant. *Id.* § 2703(b). However, in a number of circumstances, notice can be delayed for up to three months after information has been obtained. *Id.* § 2705.

name, address, phone numbers, billing records, and types of services the customer has utilized.³⁶⁶ Recently, the USA-PATRIOT Act has expanded the information that can be obtained from customer records with a subpoena to include “records of session times and durations,” “any temporarily assigned network address,” and “any credit card or bank account number” used for payment.³⁶⁷

Under Title II, a communications service provider “shall disclose a record or other information” about a customer when the government obtains a court order.³⁶⁸ A Title II court order only requires that the government provide “specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation.”³⁶⁹

One of the most important pieces of information an ISP has in its records is the customer’s identity. A customer may use a pseudonym (a screen name), and an ISP may have information linking that pseudonym to the customer’s real name. Thus, an ISP often holds the key to one’s ability to communicate anonymously on the Internet. The government often wants to obtain this information to identify a particular speaker.

For example, in *United States v. Hambrick*,³⁷⁰ a police officer served the defendant’s ISP, Mindspring, with a blatantly invalid subpoena that had been “judicially” authorized by another police officer.³⁷¹ Although the court recognized that the subpoena was invalid, the evidence was not suppressed due to Title II’s lack of an exclusionary remedy.³⁷²

In *United States v. Kennedy*, an anonymous person called an employee at Road Runner (the defendant’s ISP) and informed him that while scanning other computers on the Internet, he had discovered child pornography on the computer of the defendant, who was a Road Runner customer.³⁷³ The caller gave Road Runner the Internet Protocol (IP) address of the defendant’s computer.³⁷⁴ Road Runner then contacted the FBI.³⁷⁵ The FBI obtained a court order for the defendant’s subscriber

366. 18 U.S.C. § 2703(c)(1)(C).

367. *Id.* § 2703(c)(2), amended by USA-PATRIOT Act § 210.

368. *Id.* § 2703(c)(1)(B).

369. *Id.* § 2703(d).

370. 55 F. Supp.2d 504 (W.D. Va. 1999).

371. *Id.* at 506.

372. *See id.* at 509.

373. 81 F.Supp.2d 1103, 1106 (D. Kan. 2000).

374. *Id.*

375. *Id.*

information.³⁷⁶ Eventually this led to the defendant's conviction for possession of child pornography.³⁷⁷ The court rejected the defendant's Fourth Amendment claim based on the third party doctrine: "When the defendant entered into an agreement with Road Runner for Internet service, he knowingly revealed all information connected to [his] IP address."³⁷⁸ Instead, Title II applied, and the court concluded that the court order was defective because the government's application failed to state enough specific facts to meet Title II's requirements. However, the court noted that there was no suppression remedy for such violations.³⁷⁹

4. Pen Registers, E-mail Headers, and Websurfing

The ECPA also attempts to fill the void left by *Smith v. Maryland* by addressing pen registers and trap and trace devices. Under Title III of the ECPA, the government must obtain a court order before installing and using a pen register or trap and trace device.³⁸⁰ However, the court order merely requires that the government demonstrate that "the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."³⁸¹ In contrast to the Fourth Amendment, probable cause is not required, nor must the target be a criminal suspect. Once the government official makes the proper certification, the court must issue the order. Consequently, courts have little discretion in granting Title III orders.³⁸² Orders can last up to sixty days.³⁸³ Finally, there is no exclusionary rule for Title III violations.

The USA-PATRIOT Act of 2001 has substantially enlarged the definition of pen registers and trap and trace devices. Where before a pen register was defined as a device that records "the numbers dialed . . . on the telephone line," the new definition encompasses devices and processes that record "dialing, routing, addressing, or signaling information" for a wide variety of transmission facilities beyond telephone lines.³⁸⁴ A pen register now applies to addressing information on e-mails and to "IP addresses."³⁸⁵

376. *Id.*

377. *Id.* at 1104.

378. *Id.* at 1110.

379. *See id.* at 1111.

380. 18 U.S.C. § 3121(a) (1994).

381. *Id.* § 3123(a) (1994).

382. "Upon application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device. . . ." *Id.* § 3123 (a)(1).

383. *Id.* § 3123(c).

384. *Id.* § 3127(3), as amended by USA-PATRIOT Act § 216.

385. *Id.*

An IP address is the unique address assigned to a particular computer connected to the Internet. All computers connected to the Internet have an IP address. All websites also have an IP address. Consequently, a list of IP addresses accessed reveals the various websites that a person has visited. Because websites are often distinctively tailored to particular topics and interests, a comprehensive list of them can reveal a lot about a person's life.

5. Financial Records

Congress has filled the void created by *United States v. Miller*, which held that bank records are not protected by the Fourth Amendment. The Right to Financial Privacy Act (RFPA) requires that government officials first obtain a warrant or subpoena before accessing financial information.³⁸⁶ The subpoena merely requires a "reason to believe that the records sought are relevant to a legitimate law enforcement inquiry."³⁸⁷ The customer must be served with the subpoena prior to its service on the financial institution. Notice, however, can be delayed in a number of circumstances.³⁸⁸ When information is "relevant to legitimate law enforcement inquiry" and subpoena authority is not available to the government, the government need only submit a formal written request for the information.³⁸⁹

In addition to banks, credit-reporting agencies have detailed records for nearly every adult American consumer. Under the Fair Credit Reporting Act (FCRA) of 1970, a consumer reporting agency "may furnish identifying information respecting any consumer, limited to his name, address, former addresses, places of employment, or former places of employment, to a governmental agency."³⁹⁰ Thus, the government can simply request this information without any court involvement. If the government desires to obtain additional information contained in credit reports, it must obtain a court order or grand jury subpoena.³⁹¹ The FCRA focuses on consumer reporting agencies. Nothing in the FCRA limits the recipients of credit reports from disclosing them to the government. Credit reports about an individual are frequently supplied to a variety of entities, such as banks, creditors, landlords, and employers.

386. See 29 U.S.C. §§ 3401–22 (1994). For more information on the RFPA, see George B. Trubow & Dennis L. Hudson, *The Right to Financial Privacy Act of 1978: New Protection from Federal Intrusion*, 12 J. MARSHALL J. PRAC. & PROC. 487 (1979).

387. 29 U.S.C. § 3407.

388. *Id.* § 3409.

389. *Id.* § 3408.

390. 15 U.S.C. § 1681f (2000).

391. *Id.* § 1681b(a)(1).

Additionally, the FCRA requires a credit reporting agency to furnish the FBI with a list of all financial institutions where a person maintains an account “when presented with a written request” signed by the FBI director or designee.³⁹² This provision is limited to foreign counterintelligence investigations and to individuals believed to be foreign agents.³⁹³

Although the RFPA and FCRA protect financial information maintained by banks and credit reporting agencies, the government can obtain financial information from ISPs, employers, landlords, merchants, creditors, and database companies, among others. Therefore, financial records are protected based only on which entities possess them. Thus, the statutory regime merely provides partial protection of financial data.

6. Electronic Media Entertainment Records

The statutory regime protects records pertaining to certain forms of electronic media entertainment. Cable records are afforded a substantial amount of protection. Cable service providers maintain records about their customers, including the fee-based channels, such as HBO, to which the customer subscribes along with the pay-per-view movies a customer orders. Under the Cable Communications Policy Act (Cable Act) of 1984,³⁹⁴ a government official must obtain a court order in order to obtain cable records. The government must offer “clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case.”³⁹⁵ Further, the subject of the information can “appear and contest” the court order.³⁹⁶ This standard is more stringent than the Fourth Amendment’s probable cause and warrant requirements. However, there is no exclusionary rule under the Cable Act. The USA-PATRIOT Act has limited the Cable Act by providing that it does not apply to cable Internet service.³⁹⁷ Thus, where a cable service provider acts as an ISP, the ECPA governs, not the Cable Act.

In addition to cable records, the statutory regime also protects video tape rental records. The Video Privacy Protection Act (VPPA) of 1988,³⁹⁸ which was passed after reporters had obtained Supreme Court Justice

392. 15 U.S.C. § 1681u.

393. *See id.*

394. 47 U.S.C. § 551 (1994).

395. *Id.* § 551(h)(1).

396. *Id.* § 551(h)(2).

397. USA-PATRIOT Act § 211.

398. 18 U.S.C. § 2710 (2001).

Nominee Robert Bork's video cassette rental records, states that a video tape service provider may disclose customer records to law enforcement officials "pursuant to a warrant . . . , an equivalent State warrant, a grand jury subpoena, or a court order."³⁹⁹ Therefore, unlike the Cable Act, the level of protection under the VPPA is much less stringent.

Although the statutory regime protects the records of certain forms of electronic media entertainment, it fails to protect the records of many others. For example, records from music stores, electronics merchants, and Internet media entities are afforded no protection.

7. Medical Records

The recently promulgated federal health privacy rules, pursuant to the Health Insurance Portability and Accountability Act (HIPAA) of 1996,⁴⁰⁰ permit law enforcement officials to access medical records with a warrant, court order, or subpoena.⁴⁰¹ Health information may also be disclosed "in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person."⁴⁰² Similar to the statutes governing other records, health information can be obtained with a mere subpoena.

Not all health records, however, are covered by HIPAA. Only records maintained by health plans, health care clearinghouses, and health care providers are covered.⁴⁰³ Doctors, hospitals, pharmacists, health insurers, and Health Maintenance Organizations (HMOs) are covered, but third parties that may have medical information are not covered. Only organizations that engage in "standard transactions" under HIPAA's administrative simplification process for health insurance claims fall within the protections of the regulations.⁴⁰⁴ For example, the sale of nonprescription drugs and the rendering of medical advice by many Internet health websites are not covered by HIPAA.⁴⁰⁵ As a recent report about the limits of HIPAA has concluded:

Many Web sites offer a "health assessment" feature where users may enter all sorts of information from height and weight to drug and alcohol

399. *Id.* § 2710(b)(2)(C).

400. The regulations are published at 45 C.F.R. §§ 160–64 (2001).

401. 45 C.F.R. § 164.512(f)(1)(ii) (2001).

402. *Id.* § 164.512(f)(2).

403. *Id.* § 160.102 (2001).

404. PEW INTERNET & AMERICAN LIFE PROJECT, INSTITUTE FOR HEALTHCARE RESEARCH AND POLICY, GEORGETOWN UNIVERSITY, EXPOSED ONLINE: WHY THE NEW FEDERAL HEALTH PRIVACY REGULATION DOESN'T OFFER MUCH PROTECTION TO INTERNET USERS 6–8 (Nov. 2001).

405. *See id.* at 7.

use. . . . For example, HealthStatus.com offers free general health assessments as well as disease specific assessments to determine an individual's risk for some of the leading causes of death. . . . [B]ecause HealthStatus.com does not accept any insurance it will not be covered by the privacy rule. . . .⁴⁰⁶

Therefore, while certain health records are protected, many are not.

8. Holes in the Regime

Federal statutes provide some coverage of the void left by the inapplicability of the Fourth Amendment to records held by third parties. Although they apply to various types of information, such as communication records, financial records, entertainment records, and health records, these records are only protected when in the hands of certain third parties. Thus, the statutory regime does not protect records based on the type of information contained in the records, but protects them based on the particular types of third parties that possess them.

Additionally, there are gaping holes in the statutory regime of protection, with classes of records not protected at all. Such records include those of merchants, both online and offline. Records held by bookstores, department stores, restaurants, clubs, gyms, employers, and other companies are not protected. Additionally, all the personal information amassed in profiles by database companies is not protected.

There is a significant amount of activity on the Internet that is not covered by the ECPA, such as information collected by websites. For example, consider *In Re DoubleClick, Inc. Privacy Litigation*,⁴⁰⁷ where the court concluded that the use and access of cookies by DoubleClick did not violate the ECPA because the "DoubleClick-affiliated Web sites had consented to DoubleClick's access of plaintiffs' communications to them."⁴⁰⁸ Moreover, records maintained by Internet retailers and websites are often not considered "communications" under the ECPA.

Thus, the statutory regime is limited in its scope and has glaring omissions and gaps. Further, the statutes are often complicated and confusing, and their protection turns on technical distinctions that can leave wide fields of information virtually unprotected.

406. *Id.* at 14, 17.

407. 154 F. Supp. 2d 497, 497 (S.D.N.Y. 2001).

408. *See id.* at 511.

B. STATUTORY REGIME ARCHITECTURE: STRUCTURE

Even where the statutory regime applies, it is deficient in the procedures it adopts to regulate the government's access to third party records. The statutory regime permits information to be obtained via court order of subpoenas—a significant departure from the Fourth Amendment which generally requires warrants supported by probable cause to be issued by a neutral and detached magistrate.

Unlike warrants, subpoenas do not require probable cause and can be issued without judicial approval. Prosecutors, not neutral judicial officers, can issue subpoenas.⁴⁰⁹ According to Stuntz: “[W]hile searches typically require probable cause or reasonable suspicion and sometimes require a warrant, subpoenas require nothing, save that the subpoena not be unreasonably burdensome to its target. Few burdens are deemed unreasonable.”⁴¹⁰ According to Ronald Degnan, subpoenas are not issued “with great circumspection” and are often “handed out blank in batches and filled in by lawyers.”⁴¹¹ As Stuntz contends, federal subpoena power is “akin to a blank check.”⁴¹²

Prosecutors can also use grand jury subpoenas to obtain third party records.⁴¹³ Grand jury subpoenas are “presumed to be reasonable” and may only be quashed if “there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury investigation.”⁴¹⁴ As Stuntz observes, grand jury subpoenas “are much less heavily regulated” than search warrants:

As long as the material asked for is relevant to the grand jury's investigation and as long as compliance with the subpoena is not too burdensome, the subpoena is enforced. No showing of probable cause or reasonable suspicion is necessary, and courts measure relevance and burden with a heavy thumb on the government's side of the scales.⁴¹⁵

409. Fisher, *supra* note 238, at 152.

410. Stuntz, *supra* note 252, at 857–58.

411. Ronan E. Degnan, *Obtaining Witnesses and Documents (or Things)*, 108 F.R.D. 223, 232 (1986).

412. Stuntz, *supra* note 252, at 864.

413. Grand juries are still used in some states as well as in the federal system. See Degnan, *supra* note 411, at 229.

414. *United States v. R. Enter., Inc.*, 498 U.S. 292, 301 (1991).

415. Stuntz, *supra* note 215, at 1038.

Therefore, courts “quash or modify” subpoenas only “if compliance would be unreasonable or oppressive.”⁴¹⁶ Further, “judges decide these motions by applying vague legal standards case by case.”⁴¹⁷

Court orders under most of the statutes are not much more constrained than subpoenas. They typically require mere “relevance” to an ongoing criminal investigation, a standard significantly lower and looser than probable cause.

The problem with subpoenas and court orders is that the judiciary has very limited oversight powers. The role of the judge in issuing or reviewing subpoenas is to determine the extent of the burden of producing the evidence. With this focus, financial hardship in producing information would give courts more pause when reviewing subpoenas than the potential invasions of privacy. The role of the judiciary in court orders is also quite restricted. For example, an order to install a pen register or trap and trace device under the ECPA merely requires that the applicant certify that the information sought be relevant to an ongoing criminal investigation.⁴¹⁸ Courts cannot look beyond the certification nor inquire into the truthfulness of the facts in the application. As one court has observed, the “judicial role in approving use of trap and trace devices is ministerial in nature.”⁴¹⁹ In short, judicial involvement with subpoenas and court orders amounts to nothing more than a rubber stamp of judicial legitimacy.

In contrast, judges engage in a meaningful presearch review under the architecture of the Fourth Amendment. Stronger standards force law enforcement officials to be more careful when applying for a warrant to engage in a search.

The current statutory regime that has attempted to fill the void created by the judicial evisceration of the Fourth Amendment is inadequate because it results in the de facto watering down of the warrant and probable cause requirements of the Fourth Amendment. As warrants supported by probable cause are replaced by subpoenas and court orders supported by “articulable facts” that are “relevant” to an investigation, the role of the judge in the process is diminished to nothing more than a decorative seal of approval. In many circumstances, neither court orders nor subpoenas are required. The government can simply ask for the information. An

416. *Oklahoma Press Pub. Co. v. Walling Wage, and Hour Admin.*, 327 U.S. 186, 208–09 (1946).

417. *Stuntz*, *supra* note 252, at 867.

418. 18 U.S.C. § 3123(a).

419. *United States v. Fregoso*, 60 F.3d 1314, 1320 (8th Cir. 1995). *See also* KERR, *supra* note 309, § IV.B.

individual's privacy is protected only by the vague and toothless privacy policies of the companies holding their information.

V. RECONSTRUCTING THE ARCHITECTURE

Today, much of our personal information is finding its way into the hands of third parties. Moreover, given the Court's current conception of privacy under the Fourth Amendment, the architecture of power that regulates many of the government's information-gathering practices is increasingly that of a confusing and gap-riddled statutory regime.

One solution to fill the void is for the Court to reverse *Smith v. Maryland* and *United States v. Miller*. Although Fourth Amendment architecture is significantly more protective than that of the statutory regime, the problem of how to regulate government access to third party records is not adequately addressed by Fourth Amendment architecture alone. As discussed earlier, the principal remedy for Fourth Amendment violations is the exclusionary rule, which prevents the government from introducing improperly obtained data during a criminal prosecution. However, many information-gathering abuses often occur in the absence of prosecutions. Therefore, the exclusionary rule is not sufficiently protective.

A better architecture of power to regulate government information-gathering from third parties should be constructed. In particular, such an architecture of power should prevent the types of problems associated with government information-gathering discussed earlier in Part II.C. An architecture should address minimization, particularization, and control. First, government information-gathering should be minimized. Sweeping investigations and vast stores of personal data in the hands of government entities present significant opportunities for the problematic uses discussed earlier. Second, efforts at gathering data should be particularized to specific individuals suspected of criminal involvement. Particularization requires law enforcement officials to exercise care in selecting the individuals who should be investigated, and it prevents dragnet investigations that primarily involve innocent people. One of the most important aspects of keeping the government under control is to prevent its investigatory powers from being turned loose on the population at large. Third, government information-gathering and use must be controlled. There must be some meaningful form of supervision over the government's information-gathering activity to ensure that it remains minimized and particularized. Further, government information uses must be controlled to prevent abuses, drifts in the uses of information, and security lapses.

The aims of the architecture, however, are not the most difficult issue. Substantively, the architecture needs a scope. Which information-gathering activities should fall within the architecture's scope? Procedurally, the architecture needs a mechanism for carrying out its aims. What type of structural controls should an architecture adopt?

A. SCOPE: SYSTEM OF RECORDS

An architecture begins with substance. It must provide guidance about which information-gathering activities it governs. What is the appropriate scope of an architecture regulating government information-gathering? In particular, should the architecture cover all instances where the government gathers personal data from third parties? Restricting all information gathering from third parties would prevent law enforcement officials from gathering initial information essential in developing sufficient evidence to establish probable cause. For example, witnesses and victims are third parties that have information about the defendant. If third parties are defined broadly, then the architecture could constrain the police substantially, perhaps impeding their ability to interview people when investigating a crime.⁴²⁰

Consequently, a line must be drawn to distinguish the instances where third parties can voluntarily supply information to the government and where the government will be prohibited from accessing information or otherwise be restrained prior to procuring the data. Although we may want to prevent Amazon.com from divulging to the government the log of books a person bought, we may not want to prohibit a person's neighbor or a stranger from telling the police which books she happened to observe the person reading.

An architecture must provide guidance for where the line is drawn. One way to draw the line is to focus on the type of data involved, distinguishing between "private" and "nonprivate" information. The architecture would protect all personal information that is private. However, how is privacy to be defined? The Court has defined privacy as total secrecy. But this conception excludes most information held by third parties from the scope of protection.

Another way to define private information is to focus on "intimate" information. A number of commentators have contended that intimacy is

420. The early stages of government investigations frequently involve talking to victims, witnesses, friends, and neighbors. The police often find out about a crime when people voluntarily report suspicious activity.

the essential characteristic of privacy. For example, according to Julie Inness, “privacy’s content covers *intimate* information, access, and decisions.”⁴²¹ According to Tom Gerety, “[i]ntimacy is the chief restricting concept in the definition of privacy.”⁴²² However, what constitutes “intimate” information? Without an adequate definition, “intimate” becomes nothing more than a synonym for “private.” Commentators attempting to give substance to the word “intimacy” have defined the word too narrowly. For example, Jeffrey Reiman views intimate information as pertaining to certain kinds of loving and caring relationships.⁴²³ Much private information, such as financial and health data, however, does not pertain to these types of relationships.

The more fundamental problem with focusing on whether information is private is that privacy is a product of context, not the status of particular facts. Easy distinctions such as intimate versus nonintimate and secret versus nonsecret fail to account for the complex nature of what is considered private. Privacy is a dimension of social practices, activities, customs, and norms that are shaped by history and culture.⁴²⁴ The matters that are considered private and public have changed throughout history. Privacy is not a property of particular forms of information, since one can always lose privacy with respect to very sensitive and revealing facts about oneself. For example, the fact that a person has leprosy may be considered private information. But if that person becomes a public advocate for leprosy research and willingly announces to the public at large that she suffers from leprosy, the information is no longer private. Few would say that the fact that President Franklin Roosevelt suffered from polio remains a private matter today. Certainly, public disclosure does not eliminate the privacy of information; indeed, even information that is exposed to others may retain its private character.⁴²⁵ Nevertheless, privacy depends upon degrees of accessibility of information, and under certain circumstances, even highly sensitive information may not be private.

421. JULIE C. INNESS, *PRIVACY, INTIMACY, AND ISOLATION* 56 (1992).

422. Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 263 (1977). For other commentators adopting an intimacy conception of privacy, see Robert S. Gerstein, *Intimacy and Privacy*, in *PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY* 265 (Ferdinand David Schoeman ed. 1984), and Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood*, in *PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY*, at 300.

423. James Rachels, *Why Privacy Is Important*, in *PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY*, *supra* note 422, at 305–06.

424. See Solove, *supra* note 17, at 1129–30.

425. See Solove, *supra* note 50, at 1176–84.

Additionally, focusing on the type of information does not solve the problem of distinguishing between the neighbor's tells the police what books he sees a person reading and Amazon.com's providing the police with a complete inventory of the books the person has purchased. By attempting to draw a line based upon the type of information, these two instances would be treated similarly. Another example more radically illustrates the problem. Many would deem information about a person's genitals to be private information. Should the police be required to obtain a warrant before talking to a victim of a sexual assault about an assailant's genitals? To many this would be absurd. On the other hand, many would express serious objections if the police, without probable cause, could simply compel information about a person's genitals from treating physicians.

Further, making distinctions based on the particular status of certain forms of information fails to account for what I call the "aggregation problem." This problem is caused by the accumulation of details. A fact here or there may seem innocuous but when combined, they become more telling about that person. Similar to a Seurat painting, where a multitude of dots juxtaposed together form a picture, bits of information when aggregated paint a portrait about a person.

Another way that a line could be drawn is based upon people's expectations. Such an approach would draw from the Court's notion of "reasonable expectations of privacy." The problem with this approach, however, is that an empirical evaluation of expectations alone could gradually lead to the diminishment of privacy as more and more people come to expect that the records held by third parties can be readily obtained by the government.⁴²⁶

If a line cannot be drawn based upon the type of information involved or people's expectations of privacy, then how should the line be drawn? The answer must focus on relationships. Privacy is not independent of the relationships of which it is a part. Individuals readily share information in certain private relationships, such as the family. In particular relationships people undertake certain risks including the risk of betrayal by one with whom confidences are shared. The fact that there are expectations and

426. See *Smith v. Maryland*, 442 U.S. 735, 740–41 n.5 (1979) (noting that "where an individual's subjective expectations had been 'conditioned' by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was").

risks, however, does not mean that they must be the exclusive focus of our inquiry.

The issue is not the conceivable risk of betrayal, but rather which risks people ought to assume and which risks people should be insured against. This determination has a normative dimension. When a patient discloses an ailment to a doctor, arguably the patient assumes the risk that the doctor will disclose the information to the public. However, there are several protections against this risk. First, patient-physician confidentiality is preserved by norms of professional conduct for physicians established by ethical rules. These rules include the Hippocratic Oath, which provides: "Whatever, in connection with my professional service, or not in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret."⁴²⁷ Modern codes of medical ethics also require that physicians keep patient information confidential⁴²⁸ or risk losing their licenses for improper disclosures. Patient-physician confidentiality is also protected in court with an evidentiary privilege.⁴²⁹ Further, courts have created tort law causes of action against physicians who disclose personal information.⁴³⁰ Finally, states have passed laws that protect against the disclosure of medical information.⁴³¹ Thus, in numerous ways, the law structures the patient-physician relationship to protect against the risk of disclosure. Similarly, the law of evidence has recognized the importance of protecting the privacy of communications between attorney and client,⁴³² priest and penitent,⁴³³ husband and wife,⁴³⁴ and psychotherapist and

427. Oath and Law of Hippocrates (circa 400 B.C.).

428. See Current Opinions of the Judicial Council of the Amer. Med. Ass'n Canon 5.05 (1984) (observing that "the information disclosed to a physician during the course of the relationship between the physician and patient is confidential to the greatest possible degree").

429. See, e.g., *Jaffee v. Redmond*, 518 U.S. 1, 6-7 (1996) (recognizing psychotherapist-patient privilege and social worker-patient privilege under the Federal Rules of Evidence); GLEN WEISSENBERGER, *FEDERAL RULE OF EVIDENCE: RULES, LEGISLATIVE HISTORY, COMMENTARY AND AUTHORITY* § 501.8.

430. See, e.g., *Hammonds v. AETNA Casualty and Surety Co.*, 243 F. Supp. 793, 799 (D. Ohio 1965); *Simonsen v. Swenson*, 177 N.W. 831, 832 (Neb. 1920). Courts, however, have made exceptions in circumstances where disclosures must be made to protect the public. *Simonsen*, 177 N.W. at 832. They have even imposed tort liability when physicians or psychotherapists fail to disclose data that could lead to imminent harm. *Tarasoff v. Regents of the Univ. of Cal.*, 551 P.2d 334, 353 (Cal. 1976).

431. See, e.g., Cal. Health & Safety Code § 199.21 (prohibiting disclosure of HIV test results); N.Y. Pub. Health L. § 17 (prohibiting disclosure of minors' medical records pertaining to sexually transmitted diseases and abortion).

432. See *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981).

433. See WEISSENBERGER, *supra* note 429, at 190.

434. See *id.*

patient.⁴³⁵ Our expectations in these relationships are the product of both existing norms and the norm-shaping power of the law. As Christopher Slobogin notes, “in a real sense, we only assume those risks of unregulated government intrusion that the courts tell us we have to assume.”⁴³⁶

Therefore, the scope of the architecture should be shaped by considerations regarding social relationships. The architecture’s scope should encompass all instances when third parties share personal information (in other words, information pertaining to individuals) contained within a “system of records.” This term is taken from the Privacy Act, which defines a “system of records” as “a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”⁴³⁷ A “system of records” is used to distinguish between collecting information by speaking with specific individuals versus obtaining it through the vast stores of records held by companies.

The problems described in Part II stem from the nature of relationships with certain third parties and the problems of the government’s collection and use of personal information. Therefore, the inquiry should focus on at least two sets of relationships: relationships with the government and relationships with the third parties that possess personal information.

In relationships with the government, the focus should be on what the collective society wants the *government* to be able to know rather than whether certain matters are public or private based on the extent of their exposure to others. The Court’s conception of privacy assumes that the government stands in the same shoes as everybody else, which is clearly not the case. If we allow a loved one to read our diary, do we also want to the government to be able to read it? As Anthony Amsterdam has observed: “For the tenement dweller, the difference between observation by neighbors and visitors who ordinarily use the common hallways and observation by policemen who come into hallways to ‘check up’ or ‘look around’ is the difference between all the privacy that his condition allows and none.”⁴³⁸

435. *Jaffee*, 518 U.S. at 15.

436. Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association’s Tentative Draft Standards*, 10 HARV. J.L. & TECH. 383, 400 (1997).

437. 5 U.S.C. § 552(a)(5) (2000).

438. Amsterdam, *supra* note 326, at 404.

Indeed, the existence of Fourth Amendment limits indicates that the government stands in a different position than ordinary citizens or private sector organizations. The possibility of aggregation and the rise of digital dossiers argue in favor of regulating the government's access to information.

One cannot lose sight of the fact that an architecture of power is being developed. The focus should be on the goals of the architecture rather than on technical distinctions over whether information is intimate enough or secret enough. These questions should not derail attention from the important issue of whether government information-gathering activities present sufficient actual and potential dangers to warrant protection. The problems discussed earlier regarding information flows from the private sector to the government stem from the extensiveness of the personal information that private sector entities are gathering today. Focusing on "systems of records" targets the type of information flow that raises concern. Because the problem of modern government information-gathering is caused by the increasing dossiers maintained in private sector record systems, the architecture targets those third parties that store data in record systems.

Our relationships with the entities that maintain record systems about us differ from other social relationships. Records are a more detailed and systematic form of information gathering. Though it is possible for the government to obtain personal data by interviewing friends and others, this is minimal compared to the systematic and profound sweep of information accessible through private sector record systems. The information in records is more permanent in nature and is readily aggregated. Thus, record systems are particularly dangerous because of their extensiveness and the ease with which information can be gathered, combined, stored, and analyzed.

Further, entities that maintain systems of records collect data in a power dynamic where information disclosure is often not consensual. A person can take considerable steps to prevent a stranger from gathering data without consent. For example, a person who is overzealous in gathering information can be subject to laws prohibiting stalking or harassment.

Relationships to employers and landlords, however, are different than those with our friends, neighbors, and even strangers. Currently, employers and landlords have a substantial amount of power to gather personal information. They often stand in an unequal position to that of the individual employees or tenants. The nature of the relationship with

employers and landlords provides them with a significantly greater amount of power and control with regard to information gathering. Moreover, the law often shapes these relationships to maintain or even further this disequilibrium of power.

Relationships with merchants and communications providers might not be as directly coercive as those with the entities that govern our livelihoods and dwellings. Because these relationships are more impersonal, perhaps it should be left to the market decide this issue. If consumers demand companies that protect their information from the government, then the market will reflect these choices.

Thus far, however, the market has not been responsive to this issue. As discussed earlier, privacy policies are often vague about information flows to the government.⁴³⁹ Individuals are usually unaware of the extent to which information about them is collected.⁴⁴⁰ As Edward Janger and Paul Schwartz point out, privacy is often a nonprice term in a negotiation that people do not adequately understand. In addition, the market fails to afford sufficient incentives to correct this information asymmetry.⁴⁴¹ Further, private sector entities have never established a relationship with the people whose data they have collected.

Even if people are informed, they have little choice but to hand over information to third parties. Life in the Information Age depends upon sharing information with a host of third party entities including phone companies, ISPs, cable companies, merchants, financial entities, medical and insurance providers, and so on. The Supreme Court in *Smith* and *Miller* has suggested that if people want to protect privacy, they should not share their information with third parties. However, refraining from doing so may result in people living as Information Age hermits, without credit cards, banks, Internet service, phones and television. The market does not seem to offer a wide array of choices for people on the basis of the amount of privacy they would like to protect. People rarely seem to bargain about privacy policies, especially provisions about sharing information with the government. The policies are not individually negotiated, but are one-size-fits-all. According to Schwartz, this state of affairs is caused by the problem of “bounded rationality” in which people, “when faced with standardized terms, . . . frequently accept whatever industry offers

439. See *supra* Part II.B.

440. Solove, *supra* note 7, at 1427–28.

441. Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1241–42 (2002).

them.”⁴⁴² Given the current state of affairs, there is little hope that the market will achieve adequate protection alone.

Therefore, the scope of the architecture must be defined broadly to encompass any third party that maintains a “system of records.” This definition of scope is not perfect, and there may be hard cases that call for exceptions. However, this rule would provide clear guidance to law enforcement officials when gathering information from third parties. This clarity is a virtue. Unlike the existing statutory architecture, which is complicated and often full of notable gaps, this architecture has clear and simple boundaries.

B. STRUCTURE: REGULATED SUBPOENAS

Many different procedural mechanisms are available to control government information gathering. These mechanisms fall on a spectrum from no control over information-gathering on one end to complete restriction of it on the other. In the middle of the spectrum are mechanisms of oversight—where the government can access information only upon making certain showings before a neutral and external party who must authorize the access.

On the “no control” end of the spectrum, private sector entities may voluntarily disclose personal information to the government. If it so desired, Amazon.com could connect its computers to those of the FBI. If a private sector entity does not volunteer information, then the government can compel its production with a mere subpoena. The entity need not contest the subpoena or provide notice to the person to whom the information pertains. Whether the entity does so would be left up to market forces—to contracts between the entity and the consumer or privacy policies.

On the other end of the spectrum are architectural mechanisms of restriction—prohibitions on government collection and use of information. These mechanisms are embodied in the architecture of the Fifth Amendment and certain evidentiary privileges. The Fifth Amendment provides that “[n]o person . . . shall be compelled in any criminal case to be a witness against himself.”⁴⁴³ The Fifth Amendment’s “privilege against self-incrimination” prevents the government from compelling individuals to testify against themselves, and completely bars use of the information

442. Schwartz, *Internet Privacy and the State*, *supra* note 6, at 822–23.

443. U.S. CONST. amend V.

obtained in violation of the right at trial. In contrast, under the Fourth Amendment architecture, evidence is admissible at trial so long as the government obtains it pursuant to a valid search warrant.

The architecture of evidentiary privileges resembles in many respects the architecture of the Fifth Amendment, because privileges bar access to certain evidence altogether. Evidentiary privileges not only restrict the ability to obtain true information, but also the ability to present it at trial. As a result, privileges are sparingly recognized. For example, when independent prosecutor Kenneth Starr subpoenaed Monica Lewinsky's mother to testify against her daughter in front of a grand jury, there was a large public outcry at the tactic.⁴⁴⁴ Although in many states, spouses may refuse to testify against each other in a criminal trial about confidential information that is known to the spouse,⁴⁴⁵ most jurisdictions refuse to recognize a similar privilege for parents and children.⁴⁴⁶

For certain relationships, complete restriction is necessary to protect the relationship. Where privacy is essential to the functioning of relationships that have a high social value, then the architecture of privileges is highly protective. Certain relationships depend upon the revelation of information. Privileges protect against "the general evil of infusing reserve and dissimulation, uneasiness, and suspicion and fear, into those communications which must take place."⁴⁴⁷ As one court has noted, "by prearrangement with a criminal suspect's priest, minister or rabbi, psychiatrist or other physician, or lawyer, the police could obtain information of great value in combating crime. The only question is whether the price would be too high."⁴⁴⁸ Certainly not all relationships that depend upon privacy are worth protecting. For example, criminal conspirators need privacy, but we do not consider the protection of these relationships to be socially beneficial. It is only those relationships that are important to society—such as the attorney-client and patient-physician relationships—that are protected by mechanisms of restriction.

Often, however, privacy is not essential to the relationship's existence, but is implicated in it. Exchange of information is incidental to most

444. Ruth Marcus, *To Some in the Law, Starr's Tactics Show a Lack of Restraint*, WASH. POST, Feb. 13, 1998, at A1.

445. *Trammel v. United States*, 445 U.S. 40, 49–50 (1980). However, a spouse can waive the right to refuse to testify, and, if so, the defendant spouse cannot prevent his or her spouse from testifying. *Id.* at 52–53.

446. *In re Grand Jury*, 103 F.3d 1140, 1146 (3d Cir. 1997) (observing that most federal and state courts have rejected the privilege).

447. *Pearse v. Pearse*, 63 Eng. Rep. 950, 957 (1846).

448. *United States v. Neal*, 532 F. Supp. 942, 946 (D. Colo. 1982).

commercial transactions and employment relationships. Adopting mechanisms of restriction to these relationships would herald a return to the regime of *Boyd v. United States*.⁴⁴⁹

In *Boyd*, the Court held that the Fourth and Fifth Amendments prevented the government from issuing a subpoena to obtain a person's private papers.⁴⁵⁰ Later, in *Gouled v. United States*,⁴⁵¹ the Court held that search warrants could not be used to gain access to one's "house or office or papers" merely to obtain evidence to use against that person in a criminal proceeding.⁴⁵² Under the rationale of *Boyd* and *Gouled*, the government could seize papers if they were instrumentalities of a crime or illegal contraband but not if they were merely evidence of a crime. This rule became known as the "mere evidence" rule.

The *Boyd* and *Gouled* regime has long been dismantled. The mere evidence rule was overturned in *Warden v. Hayden*,⁴⁵³ where the Court eliminated the rule and permitted searches to find evidence of crimes.⁴⁵⁴ Moreover, the Fifth Amendment was virtually eliminated as a protection against government access to personal information in records. In *Shapiro v. United States*,⁴⁵⁵ the Court held that requiring a person to produce required records did not violate the Fifth Amendment. In *Couch v. United States*,⁴⁵⁶ the government issued a subpoena to the defendant's accountant to obtain documents pertaining to its investigation of tax fraud.⁴⁵⁷ The defendant challenged the subpoena on the basis that it violated his Fifth Amendment right against compulsory self-incrimination.⁴⁵⁸ The Court rejected the challenge reasoning that "the Fifth Amendment privilege is a *personal* privilege: it adheres basically to the person, not to information that may incriminate him."⁴⁵⁹ Because the subpoena was issued on a third party, "[i]nquisitorial pressure or coercion against a potentially accused person, compelling her, against her will, to utter self-condemning words or produce incriminating documents is absent."⁴⁶⁰ Likewise, in *Fisher v.*

449. 116 U.S. 616 (1886).

450. *See id.* at 638.

451. 255 U.S. 298 (1921).

452. *Id.* at 309.

453. 387 U.S. 294 (1967).

454. *See id.* at 309–10.

455. 335 U.S. 1 (1948).

456. 409 U.S. 322 (1973).

457. *See id.* at 323.

458. *See id.*

459. *Id.* at 328.

460. *Id.* at 329.

United States,⁴⁶¹ the Court held that the Fifth Amendment privilege did not apply to subpoenas issued upon a person's attorney.⁴⁶² The Fifth Amendment, reasoned the Court, "protects against compelled self-incrimination, not the disclosure of private information."⁴⁶³ In other words, according to the Court, the Fifth Amendment could not "serve as a general protector of privacy" and was limited to protecting against only the compulsion to testify against oneself.⁴⁶⁴

Resurrecting the "mere evidence" rule and applying it to third party records would effectively bar the government from seeking and using records entirely unless they were the very instrumentalities through which a crime was perpetrated. This would cripple modern criminal investigation. As Stuntz observes: "Government regulation require[s] lots of information, and *Boyd* came dangerously close to giving regulated actors a blanket entitlement to nondisclosure. It is hard to see how modern health, safety, environmental, or economic regulation would be possible in such a regime."⁴⁶⁵ Because *Boyd* rested in part on the Fifth Amendment, it completely prevented the government from obtaining and using the papers against the defendant no matter what procedure the government had used to obtain them.

In the middle of the spectrum are mechanisms of oversight. An architecture containing this type of mechanism is preferable to regulate government access of records held by third parties maintaining "systems of records." Mechanisms of oversight allow the government to gather information by making adequate showings before a neutral detached party. Oversight is embodied in the Fourth Amendment's *per se* warrant rule. The warrant requirement achieves the aims of minimization, particularization, and control. Collection is minimized by the requirement that the government justify that its information gathering is legitimate and necessary. The warrant ensures particularization with its requirement that there be probable cause that a particular person be engaged in criminal activity. Finally, the warrant achieves control (at least over the collection efforts) by having a neutral and detached party authorize the collection.

In many cases, warrants are the best regulatory device for government information-gathering. Often, at the point during an investigation that certain information from third parties becomes important for law

461. 425 U.S. 391 (1976).

462. *See id.* at 414.

463. *Id.* at 401 (internal quotations and alterations omitted).

464. *Id.*

465. Stuntz, *supra* note 215, at 1050.

enforcement officials to obtain, there is already enough evidence to support a warrant. In both *Smith* and *Miller* there was probably sufficient evidence for the police to secure warrants. Therefore, the requirement of a warrant hopefully prevents cases of illegitimate abuses such as large-scale information sweeps and investigations without particularized suspicion, without unduly interfering with legitimate law enforcement activities. Further, third party records have few of the dangers that make warrants inefficient. For example, because third parties maintain the records, there are fewer opportunities for a suspect to hide or destroy documents during the time law enforcement officials obtain a warrant.

However, as discussed above, merely applying the Fourth Amendment to government access to private sector records proves inadequate. First, is difficult to incorporate the “system of records” scope into the Fourth Amendment’s reasonable expectations of privacy approach to determining the scope of protection. Second, the exclusionary rule only provides a remedy at trial, and many of the abuses associated with government information-gathering extend far beyond criminal trials.

Despite being far more permissive for government information-gathering purposes, subpoenas have certain protections not available with search warrants. Unlike warrants, they can be challenged prior to the seizure of the documents. The subpoenaed party can refuse to comply and make a motion to quash before a judge. Further, subpoenas permit the target to produce the documents rather than have government agents rummage through the party’s home or belongings.⁴⁶⁶ The advantages of subpoenas over search warrants are best illustrated in *Zurcher v. The Stanford Daily*,⁴⁶⁷ where the police searched a newspaper’s offices for evidence relating to a criminal suspect. The newspaper was not involved in the alleged crime; it merely possessed evidence. The Court upheld the search because it was made pursuant to a valid warrant. Dissenting justices contended that there were First Amendment concerns with such searches because they would disrupt newspaper operations and result in “the possibility of disclosure of information received from confidential sources, or of the identity of the sources themselves.”⁴⁶⁸ Congress responded to *Zurcher* by passing the Privacy Protection Act of 1980,⁴⁶⁹ which restricts the use of search warrants for offices of newspapers and other media

466. Fisher, *supra* note 238, at 151.

467. 436 U.S. 547 (1978).

468. *Id.* at 571.

469. Pub. L. No. 96-440, 94 Stat. 1879, codified at 42 U.S.C. § 2000aa (1994).

entities for evidence of crimes of other parties. In effect, the Act requires the use of subpoenas rather than warrants to obtain such evidence.

The benefits of subpoenas, however, often do not apply to subpoenas for an individual's records issued on third parties because the third party does not need to notify the target or may not have any incentive to challenge the subpoena in court.⁴⁷⁰ Further, as discussed before, subpoenas have many weaknesses compared to warrants, such as a lack of requiring particularized suspicion and little protection by way of oversight by the judiciary.⁴⁷¹

Therefore, the Fourth Amendment architecture should be resurrected statutorily, by heightening the standards required for the government to obtain a subpoena or court order. In this way, the statutory regime could require more stringent requirements for subpoenas and court orders, such as notice to the target and particularized suspicion. In other words, subpoenas and court orders could be strengthened to resemble warrants. This statutory regime would incorporate the exclusionary rule, a minimum statutory damages provision, and a framework by which to discipline offending law enforcement officials.

If subpoenas are not made identical to warrants, an alternative structural device, a "regulated subpoena," could be used. A regulated subpoena would be similar to a warrant. It would require notice to the third party from whom the records are sought and to the subject of the records being searched so that they may be able to contest the subpoena. In certain exigent circumstances, there may be exceptions to notice, as there are currently for warrants.⁴⁷²

The regulated subpoena would require probable cause that the suspect is engaged in criminal activity. Specific records need not directly contain evidence of criminal activity but must be of "material importance" to the investigation. This differs from the standards often used by the statutory regime for subpoenas and court records in two respects. First, unlike the existing court order standard, where the person to whom the records pertain need not be involved in criminal activity at all, the regulated subpoena requires that the government demonstrate probable cause that the person is engaged in criminal activity. Second, unlike "relevance," the standard of

470. Some states, such as California, have enacted laws requiring the notification of the people to whom the records pertain. See CAL. CODE CIV. PROC. § 1985.3; Degnan, *supra* note 411, at 233.

471. See *supra* Part IV.B.

472. I am not contending that all of the existing exceptions to notice are valid; rather, I believe that some of these exceptions are acceptable.

“material importance” is narrower. It is slightly more permissive than that of a warrant, which requires that the records contain evidence of criminal activity. However, unlike a warrant, the regulated subpoena can be challenged in court.

This approach is similar to courts’ imposing heightened requirements when private parties seek to subpoena the identities of anonymous speakers. Consider, for example, *Doe v. 2TheMart.com*,⁴⁷³ where the court held that a subpoena for the identities of anonymous speakers requires heightened standards to protect the right to speak anonymously.⁴⁷⁴ According to the court, four factors determine whether a subpoena can be issued:

(1) the subpoena seeking the information [must be] issued in good faith and not for any improper purpose, (2) the information sought relates to a core claim or defense, (3) the identifying information is directly and materially relevant to that claim or defense, and (4) information sufficient to establish or disprove that claim or defense is unavailable from other sources.

Other courts have articulated similar tests.⁴⁷⁵ Even based on existing law, government subpoenas that compel information to reveal the identity of an anonymous speaker would seemingly fall within the reasoning of these courts and require heightened standards. However, a regulated subpoena would apply beyond situations where information is likely to affect anonymous speech to other forms of personal information.

The regulated subpoena requirement would contain certain exceptions. The general rule is that third parties maintaining personal information in a “system of records” cannot voluntarily disclose information to the government. Under compelling circumstances, however, third parties maintaining systems of records should be able to disclose facts voluntarily to the government. Compelling circumstances might include an imminent threat of harm to another. Another exception would allow the individual to whom the records pertain to authorize the government to obtain them from the third party without having to meet the heightened standards of the regulated subpoena. For example, if a victim of computer hacking wanted to permit the government to access the victim’s ISP records, the victim could authorize the government to do so.

473. 140 F. Supp.2d 1088 (W.D. Wash. 2001).

474. *Id.* at 1089–93.

475. *See, e.g.,* Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999).

Whether by reversing the third party doctrine, imposing Fourth Amendment restrictions on subpoenas, or restricting subpoenas via statute, the important point is that all of these approaches incorporate some of the central aspects of Fourth Amendment architecture: requiring a limitation in scope of the information that may be obtained and requiring meaningful external oversight.

C. REGULATING POST-COLLECTION USE OF DATA

The procedural architectural features discussed in the previous section are not sufficient to afford adequate protection to privacy. Another problem that must be addressed is the way personal information is used once it has been collected. As Stuntz astutely observes: “Fourth Amendment law regulates the government’s efforts to uncover information, but it says *nothing* about what the government may do with the information it uncovers. Yet as the Clinton investigation shows, often the greater privacy intrusion is not the initial disclosure but the leaks that follow.”⁴⁷⁶ Carol Steiker notes: “Unlike other countries in North America and Western Europe, the United States [has] never developed a national plan to organize a ‘system’ of policing or to provide for centralized control over police authority.”⁴⁷⁷ Once information is collected, the Fourth Amendment’s architecture of oversight no longer applies. This is problematic, as many of the abuses of information by the government discussed earlier occur after the information has been collected.

The Privacy Act of 1974⁴⁷⁸ provides some limited regulation of records maintained by government law enforcement entities. However, the Act contains many exceptions and loopholes that have limited its effectiveness. Government entities can share information widely with each other. Further, information may be disclosed for any “routine use,” an exception that many have criticized as a significant loophole.⁴⁷⁹ As Robert Gellman astutely observes, the Privacy Act provides a “vague standard” that fails to serve as “a significant barrier to the sharing of personal information within agencies.”⁴⁸⁰ Additionally, the Act applies only to the federal government. Fewer than a third of the states have a privacy law similar to the Privacy Act.⁴⁸¹

476. Stuntz, *supra* note 252, at 857.

477. Steiker, *supra* note 121, at 834.

478. 5 U.S.C. § 552a (2000).

479. See, e.g., Schwartz, *supra* note 5, at 585–86.

480. Gellman, *supra* note 141, at 198.

481. Solove, *supra* note 50.

The Privacy Act is an important first step in reigning in the vast stores of data that government entities collect. There remains, however, much room for the Privacy Act to be improved and strengthened. One possible way to provide a safeguard is to mandate the destruction of data after certain periods of time or, mandate the transfer of data to the judicial branch, after a certain period of time, for access only under special circumstances. Another way is to adopt a meaningful-purpose specification restriction. This means that, with certain reasonable exceptions, information collected from third party records may only be used for the particular purpose for which it is collected.

VI. CONCLUSION

One of the most significant threats to privacy of our times, government information-gathering and-use, is inadequately regulated. The Court's Fourth Amendment jurisprudence has been mired in the difficulties of conceptualizing privacy, thus preventing the application of the Fourth Amendment. A statutory regime has arisen to fill the void, but it is severely flawed. A new architecture of power must be constructed, one that effectively regulates the government's collection and use of third party records. This task is not easy in a rapidly changing society that is adjusting to the profound new dimensions of the Information Age. This Article is thus a beginning of the process.

