SUFFOLK UNIVERSITY
LAW REVIEW

Volume XLVII 2014 Number 2

The Constitutional Protection of Information in a Digital Age

Gerard J. Clark*

TABLE OF CONTENTS

* Professor of Law, Suffolk University Law School.

I. INTRODUCTION

To state the obvious, we live in a world that is awash in information. Discoveries of new scientific information occur daily in the laboratories of the world. The Facebook accounts of millions of teenagers contain information about the love lives of their friends. Google traces the search information of its subscribers.[1] Supermarkets use personalized discount cards to trace the purchasing preferences of their customers.[2] The National Security Agency (NSA) has been building a one-million-square-foot data and supercomputing center in Utah, which is expected to intercept and store much of the world's Internet communication for decryption and analysis.[3] States maintain driver, tax, and voter records. All of these records contain information that can yield profit for some and embarrassment for others.

The First Amendment to the U.S. Constitution dictates access to and dissemination of this information, whereas the Fourth Amendment limits such access and dissemination. Additionally, common-law doctrines of privacy, publicity, and defamation apply to this information, as do copyright, patent, and trademark law. State and federal legislatures race to regulate the collection, storage, and dissemination of this data and information in the public interest. This Article will review recent developments in the constitutional treatment of access to data and information, will comment on an illustrative group of statutory and common-law developments, and will discuss a number of current noteworthy controversies.

II. FIRST AMENDMENT PROTECTION OF INFORMATION

The First Amendment is often invoked to test the legitimacy of a governmental restriction on the free flow of information in society. For example, early cases from the World War I era involved criminal prosecutions against identified speakers whose messages were claimed to undermine the war effort.[4] In the 1950s, advocates of communism were prosecuted for holding a political philosophy at odds with the legitimacy of the American government.[5]

1. *See Privacy Policy*, GOOGLE, www.google.com/policies/privacy (last modified Dec. 20, 2013) (relaying search queries automatically collected and stored in server logs).

2. *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES, Feb. 16, 2012, http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all&_r=0 (explaining how retailers collect information about their consumers).

3. *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1934 (2013) (citing James Bamford, *The Black Box*, WIRED, Apr. 2012, at 78, 80) (describing construction and purpose of new NSA data facility).

4. *See, e.g.*, Abrams v. United States, 250 U.S. 616, 624 (1919) (affirming convictions for inciting resistance to war effort); Frohwerk v. United States, 249 U.S. 204, 210 (1919) (affirming conviction for willful obstruction in war recruitment efforts); Schenck v. United States, 249 U.S. 47, 53 (1919) (affirming convictions for distributing antiwar leaflets to men called for military service).

5. *See* Yates v. United States, 354 U.S. 298, 333-34 (1957) (dismissing convictions for membership in

More modern First Amendment concerns, however, are less about closing the mouths of dissidents and more about policing legislative and bureaucratic limitations on the movement of information or data.[6] The speakers in these cases may be machines, and the information may be in digital form. Data miners face obstacles in gaining access to the information, while individuals seek to shield their personal information from such data miners.

A. Recent Case Law

In *Sorrell v. IMS Health Inc.*, the Supreme Court broke new ground by holding that data miners have a First Amendment right to demand access to data compiled pursuant to a state regulatory program in order to package and sell it for commercial purposes.[7] The Court invalidated a Vermont statute that restricted the sale, disclosure, and use of pharmacy records that reveal the prescribing practices of individual doctors to pharmaceutical manufacturers for marketing purposes.[8] The plaintiffs, three Vermont data miners and an association of pharmaceutical manufacturers that produce brand-name drugs, brought this anticipatory attack to invalidate the statute.[9]

In 2007, Vermont enacted the Prescription Confidentiality Law (Act 80).[10] Act 80 provided, among other things, that "[a] health insurer, a self-insured employer, an electronic transmission intermediary, a pharmacy, or other similar entity shall not sell, license, or exchange for value regulated records containing prescriber-identifiable information, nor permit the use [of such records] . . . for marketing or promoting a prescription drug, unless the prescriber consents . . . ."[11] In addition, Act 80 stated that "[p]harmaceutical manufacturers and pharmaceutical marketers shall not use prescriber-identifiable information for marketing or promoting a prescription drug unless the prescriber consents . . . ."[12] The statute contained a number of exceptions for health care research, enforcing compliance with insurance formularies, care-management educational communications sent to patients about their conditions, law

Communist Party), *overruled on other grounds by* Burks v. United States, 437 U.S. 1 (1978); Dennis v. United States, 341 U.S. 494, 516-17 (1951) (upholding conviction for conspiring to organize Communist Party in United States).

6. *See generally* Sorrell v. IMS Health Inc., 131 S. Ct. 2653 (2011) (considering whether data mining physician-prescription information for marketing purposes constitutes commercial speech).

7. *See id.* at 2672 (holding prohibition on using prescription information for marketing-specific content and speaker-based restrictions).

8. *See id.*

9. *See id.* at 2661.

10. *Sorrell*, 131 S. Ct. at 2660; Act of June 9, 2007, No. 80, § 17, 2007 Vt. Acts & Resolves 635, 657 (codified at VT. STAT. ANN. tit. 18, § 4631 (2011)), *invalidated by* Sorrell v. IMS Health Inc., 131 S. Ct. 2653 (2011).

11. tit. 18, § 4631(d).

12. *Id.*

enforcement operations, and other purposes provided by law.[13] Moreover, Act 80 authorized funds for an "evidence-based prescription drug education program."[14]

Act 80 was accompanied by a number of legislative findings.[15] Vermont found, for example, that pharmaceutical marketing program goals are often in conflict with state goals, and that the "marketplace for ideas on medicine safety and effectiveness is frequently one-sided in that brand-name companies invest in expensive pharmaceutical marketing campaigns to doctors."[16] Detailing, in the legislature's view, results in doctors making decisions based on incomplete and biased information.[17] Because Vermont doctors do not have time to research the quickly changing pharmaceutical market, the legislature found that they rely on information provided by pharmaceutical representatives.[18]

The Court's primary objection to the Vermont statute was that on its face, the law enacted content-based and speaker-based restrictions on the sale, disclosure, and use of prescriber-identifying information.[19] As drafted, the statute disfavors marketing, that is, speech with a particular content and specific speakers—namely pharmaceutical manufacturers.[20] Because the law places these categorical restrictions on speech, the Court applied the intermediate test for commercial speech.[21] In order for a state to sustain such

13. *Id.* § 4631(e).

14. *See* § 14, 2007 Vt. Acts & Resolves at 649. One of the program's aims is to advise prescribers about common brand-name drugs for which the patent has expired or will soon expire. *See* tit. 18, § 4622(a)(2). Efforts promoting the use of generic drugs are sometimes referred to as "counter-detailing." *See* Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2661 (2011).

> [C]ounterdetailer's recommended substitute may be an older, less expensive drug and not a bioequivalent of the brand-name drug the physician might otherwise prescribe. Like the pharmaceutical manufacturers whose efforts they hope to resist, counterdetailers in some States use prescriber-identifying information to increase their effectiveness. States themselves may supply the prescriber-identifying information used in these programs.

Id.

15. *See* § 1, 2007 Vt. Acts & Resolves at 635-39.

16. Act of June 9, 2007, No. 80, § 1(3)-(4), 2007 Vt. Acts & Resolves 635, 635.

17. *See id.* § 1(4).

18. *See id.* § 1(13). The Vermont legislature further found that detailing increases the cost of medications and individuals' healthcare budgets, encourages hasty and excessive reliance on brand-name drugs as compared to older and less expensive generic alternatives, and fosters disruptive and repeated marketing visits tantamount to harassment. *See id.* § 1(7), (15), (27)–(28). The legislative findings also noted that the effectiveness of detailing programs is bolstered by the use of prescriber-identifying information because it allows detailers to target their visits to particular doctors. *See id.* § 1(23)–(26). Additionally, prescriber-identifying data helps detailers shape their messages by tailoring "presentations to individual prescriber styles, preferences, and attitudes." *Id.* § 1(25).

19. *See Sorrell*, 131 S. Ct. at 2663.

20. *See* Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2663 (2011) ("Vermont's law thus has the effect of preventing detailers—and only detailers—from communicating with physicians in an effective and informative manner.").

21. *See id.* at 2664; *see also* Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 658 (1994) ("[S]peaker-

restrictions under the intermediate test, the state must show that the law in question advances substantial government interests, and that the law is directly aimed at achieving such interests.[22]

Vermont asserted two justifications for Act 80's restrictions on speech.[23] First, it argued that the restrictions were "necessary to protect medical privacy, including physician confidentiality, avoidance of harassment, and the integrity of the doctor-patient relationship."[24] Second, it claimed the restrictions were integral to the objectives of improving public health and reducing healthcare costs.[25] The Court rejected both justifications, thereby validating the data miners' claim to access the records mandated by the statute that contained every physician's prescription practices.[26]

Although the Court in *Sorrell* rejected Vermont's interest in protecting the privacy of physician-prescribing practices, other privacy interests and claims have been successful. For instance, the First Amendment protects a speaker from dangers that may eventuate from disclosure of his identity.[27] In *NAACP v. Alabama*, the Alabama Attorney General issued a demand on the NAACP to reveal the names and addresses of all of its Alabama members and agents.[28] The demand was made in connection with efforts to enforce a statute requiring registration of foreign corporations seeking to do business in Alabama.[29] When the NAACP refused to comply, a state trial court held the association in contempt and fined it $100,000.[30] In an opinion authored by Justice Harlan, the Court recognized that a vital relationship exists between the freedom to associate and the privacy in one's associations, and held that the right to pursue lawful interests privately is constitutionally protected.[31]

based laws demand strict scrutiny when they reflect the Government's preference for the substance of what the favored speakers have to say (or aversion to what the disfavored speakers have to say)."); Cincinnati v. Discovery Network, Inc., 507 U.S. 410, 416-18 (1993) (employing heightened scrutiny in reviewing categorical prohibition on using news racks for distributing commercial messages). The Court first recognized First Amendment protection for the free flow of commercial information, including advertising, in *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council*. *See* 425 U.S. 748, 756-57 (1976) ("If there is a [First Amendment] right to advertise, there is a reciprocal right to receive the advertising . . . .").

22. *See Sorrell*, 131 S. Ct. at 2667-68; *see also* Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 566 (1980) (outlining four-part analysis for commercial-speech cases).

23. *Sorrell*, 131 S. Ct. at 2668.

24. *Id.*

25. *See id.* at 2668.

26. *See* Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2668-71 (2011) (stating rationale for rejection of justifications advanced by state). The First Circuit reached a contrary result when reviewing a similar statute enacted in New Hampshire. *See* IMS Health Inc. v. Ayotte, 550 F.3d 42, 53 (1st Cir. 2008) (opining statute principally regulated conduct not speech), *abrogated by* Sorrell v. IMS Health Inc., 131 S. Ct. 2653 (2011).

27. *See* NAACP v. Alabama, 357 U.S. 449, 466 (1958) (applying First Amendment to states through due process clause of Fourteenth Amendment, and implicitly holding freedom of association falls under First Amendment).

28. *See id.* at 453.

29. *See id.* at 451-52.

30. *See id.* at 454.

31. *See NAACP*, 357 U.S. at 466.

In *Doe v. Reed*, the petitioners sought to prevent public disclosure of their support for a ballot initiative opposing recognition of gay marriage in the State of Washington.[32] Protect Marriage Washington, the citizens group that sponsored the referendum petition, attempting to revoke a recently enacted statute extending benefits to same-sex marriages, claimed that releasing the names of those who signed the petition violated the First Amendment.[33] The petition included the names and addresses of the signatories, and was submitted to the secretary of state for verification and canvassing to ensure that only lawful signatures were counted.[34] Washington's Public Records Act (PRA) permits private parties to obtain copies of state government documents, and Washington took the position that the PRA encompasses documents submitted in connection with referendum petitions.[35]

Protect Marriage Washington and certain referendum petition signatories sought an injunction against the release of the petition documents containing individuals' names, alleging fear of "threats, harassment, and reprisals."[36] The Court held that the signatory information on the referendum petition was expressive under the First Amendment.[37] Further, the Court recognized that the PRA was not being used to prohibit speech, but rather was a disclosure requirement.[38] The Court held that "the State's interest in preserving the integrity of the electoral process suffices to defeat the argument that the PRA is unconstitutional with respect to referendum petitions . . . ."[39]

The above-mentioned cases illustrate, unsurprisingly, that the privacy

> It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association as the forms of governmental action in the cases above were thought likely to produce upon the particular constitutional right there involved. This Court has recognized the vital relationship between freedom to associate and privacy in one's associations.

Id. at 462.

32. *See* 130 S. Ct. 2811, 2816 (2010).

33. *See id.* at 2817.

34. *See id.* at 2816. Washington Governor Christine Gregoire originally enacted the legislation in question in May 2009. *See id.* By July 2009, Protect Marriage Washington obtained a sufficient number of signatures to place their referendum on the ballot. *See id.* In November 2009, voters approved the legislation enacted by the governor by a margin of fifty-three to forty-seven percent. *See id.*

35. *See id.* The PRA makes all "public records" available for inspection and copying. *See* WASH. REV. CODE ANN. § 42.56.070(1) (West 2013). The Act defines a "public record" as "any writing containing information relating to the conduct of government or the performance of any governmental or proprietary function prepared, owned, used, or retained by any state or local agency . . . ." *Id.* § 42.56.010(3).

36. *Reed*, 130 S. Ct. at 2816 (recounting allegations within injunctive complaint).

37. *See id.* at 2818 (stating expression of political views implicates First Amendment rights).

38. *See* Doe v. Reed, 130 S. Ct. 2811, 2818 (2010); *see also* Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 366 (2010) ("Disclaimer and disclosure requirements may burden the ability to speak, but they . . . 'do not prevent anyone from speaking.'" (quoting McConnell v. Fed. Election Comm'n, 540 U.S. 93, 201 (2003))).

39. *Reed*, 130 S. Ct. at 2819.

principle embedded in the First Amendment is weak and narrow. Certainly, if disclosure of membership could lead to a lynching, the First Amendment will not mandate the disclosure of an association with a disfavored group. However, the decision in *NAACP v. Alabama* does not speak to validating unsubstantiated fears that homosexuals will target heterosexuals in the State of Washington. Moreover, the First Amendment forced disclosure in *Sorrell*. There the claims in favor of nondisclosure at the behest of the State on behalf of prescription writers failed. As discussed *infra*, the Fourth Amendment typically provides a stronger claim for nondisclosure of such individually identifiable information.[40]

In *McIntyre v. Ohio Elections Commission*, the Court established a right to speak anonymously.[41] The defendant in *McIntyre* distributed leaflets at a public meeting expressing opposition to a school tax levy.[42] Following the passage of the tax levy in subsequent elections, a school official filed a complaint with the Ohio Elections Commission charging that McIntyre's distribution of unsigned leaflets violated Ohio law.[43] The Commission agreed and imposed a $100 fine.[44]

The Court stated that the Ohio election statute's prohibition of anonymous leaflets was a weapon against fraud and helped to deter "false statements by unscrupulous prevaricators," but that it was also too broad in its reach.[45] The Court distinguished the disclosure requirement in federal election laws stating that Ohio's infringement on speech was more intrusive and rested on different state interests.[46]

> In candidate elections, the Government can identify a compelling state interest in avoiding the corruption that might result from campaign expenditures. Disclosure of expenditures lessens the risk that individuals will spend money to support a candidate as a *quid pro quo* for special treatment after the candidate is in office.[47]

40. *See infra* Part III.A-B (discussing Fourth Amendment cases and principles regarding individual privacy).

41. *See* 514 U.S. 334, 342 (1995).

42. *See id.* at 337.

43. *See id.* at 338. The school official claimed that McIntyre violated the Ohio law prohibiting distribution of leaflets "designed to promote the defeat of any issue," without the conspicuous name of the party responsible for such notice. *See id.* at 338 & n.3 (describing then current section of applicable Ohio Code).

44. *See id.* at 338.

45. *McIntyre*, 514 U.S. at 349-51.

46. *See id.* at 356.

47. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 356 (1995). *See generally* Margot Kaminski, *Real Masks and Real Name Policies: Applying Anti-Mask Case Law to Anonymous Online Speech*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 815 (2013) (reviewing case law where claimants seek compensation against anonymous online speech).

The Court also noted in *McIntyre* that

> anonymity may be motivated by fear of . . . retaliation, by concern about social ostracism, or merely by a desire to preserve . . . one's privacy[,] . . . . [but] an author's decision to remain anonymous, like other decisions concerning . . . the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.[48]

Reed is distinguishable because the referendum petition signatures in that case were filed with the state and discoverable under Washington's PRA, and the state's interest in the integrity of the initiative process was specific and compelling. In contrast, the anonymous leaflet prohibition in *McIntyre* was general and directed at political argument, and the exclusion of all anonymous campaigning would exclude the reticent citizen's voice.[49]

Another claim for sanctions against an unauthorized disclosure arose in *Bartnicki v. Vopper*, where an unidentified person intercepted and recorded a cell phone conversation between Bartnicki, the chief union negotiator, and the union president concerning collective-bargaining negotiations between the teachers union and the school board.[50] Following the parties acceptance of a nonbinding arbitration proposal generally favorable to the teachers, Vopper, a radio commentator, played a tape of the intercepted conversation on his public affairs talk show in connection with news reports about the settlement.[51] Petitioners filed an action for damages under state and federal wiretapping laws alleging, among other things, that their conversation was "surreptitiously intercepted by an unknown person," the head of a local organization opposed to the union's demands obtained the tape and intentionally disclosed it to the media, and that the media had repeatedly published the conversation even though they knew or had reason to know that it had been illegally intercepted.[52] The Court ruled that the First Amendment protected the disclosure made by the radio station despite the illegal interception.[53]

48. *McIntyre*, 514 U.S. at 341-42.

49. *Compare id.* at 350-53 (dispelling state justifications for restriction on anonymous speech), *with* Doe v. Reed, 130 S. Ct. 2811, 2820 (2010) (preserving electoral integrity compelling enough interest to defeat unconstitutional argument on public records disclosure).

50. *See* 532 U.S. 514, 518 (2001).

51. *See id.* at 519.

52. *See id.* at 519-20.

53. *See id.* at 535 (opining illegal conduct does not remove First Amendment protection of speech on important public matters). The Court stated that "[i]n these cases, privacy concerns give way when balanced against the interest in publishing matters of public importance." *Id.* at 534. In *New York Times Co. v. United States*, the Court likewise protected the media's access to the then-classified Pentagon Papers without risk of censorship even though the documents were surreptitiously smuggled out of the Pentagon. *See* 403 U.S. 713, 714 (1971) (per curiam).

More recently, the Court appeared to be granting certiorari in unusual cases that required narrow interpretations of exceptions to First Amendment doctrine. For instance, the Court held that the First Amendment protects violent video games,[54] animal torture videos,[55] outrageous speech at an Iraq veteran's funeral,[56] lies about winning military awards,[57] and the future opinions of federal aid recipients.[58] The lower federal courts have also been active in their review of First Amendment claims against statutes and regulations designed to protect individuals against unauthorized dissemination of personal information. These cases further illustrate the tension between the values of information dissemination and individual privacy.

In *Trans Union Corporation v. Federal Trade Commission*, a credit reporting agency challenged the constitutionality of the Fair Credit Reporting Act (FCRA), which generally forbids companies from sharing consumer credit reports except for a specified list of purposes.[59] The Court of Appeals for the D.C. Circuit, assuming that the consumer reports constituted speech, held that the Act's limitations on dissemination of consumer reports did not violate the First Amendment.[60] However, the D.C. Circuit acknowledged the substantial interest in protecting the privacy of such consumer credit information.[61]

U.S. West, Inc. v. FCC presented a First Amendment challenge to a privacy regulation promulgated under § 222 of the Telecommunications Act of 1996, restricting telecommunications providers from disclosing or using customer data outside of a narrow set of purposes.[62] The regulated telecommunications data included any "information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer . . . ."[63] This expansive definition includes not only the sorts of information that the telecommunications provider records in its bills and other business records, but also data describing when,

54. *See* Brown v. Entm't Merchs. Ass'n, 131 S. Ct. 2729, 2740-42 (2011) (holding law restricting sale or rental of violent games to minors both underinclusive and overinclusive).

55. *See* United States v. Stevens, 559 U.S. 460, 482 (2010) (holding statute criminalizing depictions of animal cruelty overbroad and facially invalid under First Amendment).

56. *See* Snyder v. Phelps, 131 S. Ct. 1207, 1219 (2011) (holding antihomosexual picketing at military funeral protected by First Amendment because matter of public concern).

57. *See* United States v. Alvarez, 132 S. Ct. 2537, 2542-43 (2012) (holding statute criminalizing lying about receipt of military medal constituted content-based restriction violating First Amendment).

58. *See* Agency for Int'l Dev. v. Alliance for Open Soc'y Int'l, Inc., 133 S. Ct. 2321, 2332 (2013) (holding statute requiring recipients of federal funds to express opposition to prostitution violates First Amendment).

59. *See* 245 F.3d 809, 811-12 (D.C. Cir. 2001). *See generally* Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x (2012) (establishing parameters of permissible uses of consumer credit reports).

60. *See Trans Union Corp.*, 245 F.3d at 819.

61. *See id.* at 818.

62. *See* 182 F.3d 1224, 1230 (10th Cir. 1999) (arguing regulatory process infringes on ability to engage in commercial speech with customers); *see also* 47 U.S.C. § 222(d) (2012) (setting forth permissible uses of customer proprietary network information under Telecommunications Act of 1996).

63. *U.S. West, Inc.*, 182 F.3d at 1228 n.1.

where, and to whom a customer places a call.[64] This information is generated in the process, and for the purpose, of providing telecommunications service.[65] The Federal Communications Commission (FCC) regulation did not restrict U.S. West from making any particular communication to their customers; instead, it deprived U.S. West of a resource the company would have used to tailor the messaging to its customers.[66] In *U.S. West* the court treated accurate information (to which the potential speaker otherwise has access) as commercial speech and proceeded to invalidate the privacy provisions in the regulation because the agency could not prove they were justified by articulable and substantial privacy or competition interests.[67]

In *Glik v. Cunniffe*, the Court of Appeals for the First Circuit addressed the issue of a citizen's right to record a government agent in the performance of his duties.[68] Glik was arrested for digitally recording several police officers arresting a young man on the Boston Common using his cellular phone's camera.[69] The charges against Glik, which included violation of Massachusetts's wiretapping statute, were dismissed.[70] Glik then brought suit under 42 U.S.C. § 1983, claiming his arrest for filming the officers constituted a violation of his rights under the First and Fourth Amendments.[71] Specifically, the First Circuit considered whether there is a constitutionally protected right to videotape police carrying out their duties in public, and responded to the inquiry unambiguously in the affirmative.[72]

The court said, "It is firmly established that the First Amendment's aegis . . . encompasses a range of conduct related to the gathering and dissemination of information," and the Amendment prohibits the government from limiting the information available to the public.[73] The court further acknowledged the

64. *See id.* at 1235.

65. *See id.* at 1229. *Cf.* Trans Union LLC v. FTC, 536 U.S. 915 (2002) (Kennedy, J., dissenting) (questioning ban on use of consumer credit reports for targeted marketing).

66. *See U.S. West, Inc.*, 182 F.3d at 1230 (describing ways carriers may communicate with customers).

67. *See id.* at 1240 (rejecting agency's privacy and competition justifications for regulation); *see also* Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 569-72 (1980) (holding regulation completely banning utility company from advertising its services to customers unconstitutional).

68. *See* 655 F.3d 78, 79 (1st Cir. 2011).

69. *See id.*

70. *See id.* at 80. Massachusetts's wiretapping statute criminalizes willful interception or attempted interception of any wire or oral communication. *See* MASS. GEN. LAWS ANN. ch. 272, § 99(C)(1) (West 2013). "As the [Massachusetts] Supreme Judicial Court has noted, this statute sweeps more broadly than comparable laws in other jurisdictions, in that its prohibition is not restricted to the recording of communications that are made with a reasonable expectation of privacy." *Glik*, 655 F.3d at 86 (citing Commonwealth v. Hyde, 750 N.E.2d 963, 967-68 & n.6 (Mass. 2001)). The critical limiting term in the statute is "interception," which is defined as taking action "to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication . . . ." ch. 272, § 99(B)(4).

71. *See Glik*, 655 F.3d at 80.

72. *See id.* at 82.

73. *Id.* "[T]he First Amendment goes beyond the protection of the press and the self-expression of

government can neither limit any lawful methods of gathering the information, nor sources from which the information is derived.[74] Therefore, the court found that the filming of police officers performing their governmental duties in a public place fell comfortably within these principles, and gathering such information additionally served a cardinal First Amendment interest in protecting and promoting "the free discussion of governmental affairs."[75] The First Circuit also noted that the right to gather news does not extend solely to the media, but rather the right coexists with the public's right of access to gather information.[76]

B. The National Security Exception

In cases involving issues of national security, the Supreme Court reigns in its activism and typically defers to the executive branch or Congress. Beginning with the World War I-era espionage and sedition cases, the Court allowed convictions to stand under the vaguely worded Espionage Act of 1917, which makes it a crime to communicate information that could be used to injure the United States or to assist a foreign nation.[77] For instance, in *Abrams v. United*

individuals to prohibit the government from limiting the stock of information from which members of the public may draw." First Nat'l Bank of Bos. v. Bellotti, 435 U.S. 765, 783 (1978); *see* Stanley v. Georgia, 394 U.S. 557, 564 (1969) ("It is . . . well established that the Constitution protects the right to receive information and ideas."); *see also* Barry P. McDonald, *The First Amendment and the Free Flow of Information: Towards a Realistic Right To Gather Information in the Information Age*, 65 OHIO ST. L.J. 249, 339-56 (2004) (proposing workable solution to information gathering under First Amendment).

74. *See* Glik v. Cunniffe, 655 F.3d 78, 82 (1st Cir. 2011).

75. *Id.* (quoting Mills v. Alabama, 384 U.S. 214, 218 (1966)). The First Circuit recalled Supreme Court precedent cautioning that discretion given to law enforcement officials concerning suppression of First Amendment protections may be misused to deprive individuals of these rights. *See id.*; *see also* Gentile v. State Bar of Nev., 501 U.S. 1030, 1035-36 (1991) (observing police and prosecutors given great discretion, and therefore, public has interest in preventing abuse and misuse of that discretion). "Ensuring the public's right to gather information about their officials not only aids in the uncovering of abuses, but also may have a salutary effect on the functioning of government more generally." *Glik*, 655 F.3d at 82-83 (citations omitted); *see also* Seth F. Kreimer, *Pervasive Image Capture and the First Amendment: Memory, Discourse, and the Right To Record*, 159 U. PA. L. REV. 335, 382-83 (2011) (stating First Amendment disproves of rules vesting officials with unbridled discretion because likelihood of suppression); Lisa A. Skehill, Note, *Cloaking Police Misconduct in Privacy: Why the Massachusetts Anti-Wiretapping Statute Should Allow for the Surreptitious Recording of Police Officers*, 42 SUFFOLK U. L. REV. 981, 1004-06 (2009) (arguing preventing civilian recordings of law enforcement interactions interferes with First Amendment right to gather information). *See generally* Travis Gunn, Note, *Knowledge Is Power: The Fundamental Right To Record Present Observations in Public*, 54 WM. & MARY L. REV. 1409 (2013) (contending right to record officials in public constitutionally protected activity).

76. *See Glik*, 655 F.3d at 83.

77. *See* 18 U.S.C. § 793(d) (2012).

> Whoever, lawfully having possession of . . . information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates [such information] . . . to any person not entitled to receive it . . . . Shall be fined under this title or imprisoned . . . .

States, the Court affirmed espionage convictions for distributing leaflets advocating for revolution and anarchy.[78] The Court referred to the defendants' testimony "that they did not believe in government in any form" and that they "had no interest whatever in the government of the United States."[79] However, Justice Holmes's dissenting opinion doubted that the defendants' leaflets could produce a clear and present danger to undermine the war effort of the United States.[80] Again, in *Dennis v. United States*, the Court affirmed the conviction of Eugene Dennis, General Secretary of the Communist Party USA, under the Smith Act, which outlawed advocacy aimed at overthrowing the government by force.[81] The Court held that the First Amendment did not protect the creation of a plot to overthrow the government under the clear and present danger test.[82]

The trend continued with *Holder v. Humanitarian Law Project*, which concerned a constitutional challenge to a federal statute making it a crime to provide "'material support or resources' to certain foreign organizations that engage in terrorist activities."[83] The U.S. Secretary of State is given the authority to designate an entity a "foreign terrorist organization," and in 1997, thirty such groups were designated as such.[84] Two of those groups included the Kurdistan Workers' Party (also known as the Partiya Karkeran Kurdistan (PKK)) and the Liberation Tigers of Tamil Eelam (LTTE).[85]

The plaintiffs in *Humanitarian Law Project*, including the Humanitarian Law Project (HLP)—a human rights organization with consultative status to the

Id. § 793(d), (f).

78. *See* 250 U.S. 616, 623-24 (1919).

79. *Id.* at 618.

80. *See id.* at 628 (Holmes, J., dissenting).

81. *See* 341 U.S. 494, 516-17 (1951) (affirming convictions for conspiracy to organize Communist Party in United States); *see also* 18 U.S.C. § 2385 (2012) (proscribing willful advocacy of overthrowing any government in United States).

82. *See Dennis*, 341 U.S. at 510-11 (supporting trial court's finding that requisite danger existed).

83. *See* 130 S. Ct. 2705, 2712-14 (2010); *see also* 18 U.S.C. § 2339B (2012) (prohibiting knowing provision of material support or resources to foreign terrorist organizations). The term "material support or resources" means

> any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials.

18 U.S.C. § 2339A(b)(1) (2012).

84. *See Humanitarian Law Project*, 130 S. Ct. at 2713; *see also* 8 U.S.C. § 1189(a)(1), (d)(1) (2012) (setting forth Secretary of State's authority relative to terrorist organization designation); Designation of Foreign Terrorist Organizations, 62 Fed. Reg. 52,650, 52,650 (Oct. 8, 1997) (listing organizations designated pursuant to Secretary of State's authority).

85. *See Humanitarian Law Project*, 130 S. Ct. at 2713; Designation of Foreign Terrorist Organizations, 62 Fed. Reg. at 52,650.

United Nations—maintained that they wanted to provide support for PKK's and LTTE's humanitarian and political activities through monetary contributions, other tangible aid, legal training, and political advocacy, but they feared prosecution under the federal statute.[86] The plaintiffs argued that the proscription on providing such support to the PKK and the LTTE constituted a restriction on political speech.[87]

The Court noted that, although "material support" is not often actual speech, the statute in question was "carefully drawn to cover only a narrow category of speech to . . . foreign groups that the speaker knows to be terrorist organizations."[88] The Court acknowledged that the parties agreed that the government's interest in combating terrorism was "an urgent objective of the highest order."[89] Notwithstanding this agreement, the plaintiffs claimed that the objective of combating terrorism did not justify the prohibition on their speech because their support of the PKK and LTTE would advance only the legitimate activities of the organizations and not their terrorism.[90] In rejecting plaintiffs' argument, the Court relied on affidavits from the U.S. State Department stating that such support would free up "other resources within the organization that may be put to violent ends."[91]

C. Statutes and Common-Law Remedies

Both state and federal statutes and regulations generally expand access to information. Enacted in 1966, the Freedom of Information Act (FOIA) provides a general right to obtain access to federal agency records, subject to nine exemptions.[92] FOIA covers the executive branch of the federal government and any executive agency that makes decisions and is essentially controlled by the federal government; however, neither Congress (the

86. *Humanitarian Law Project*, 130 S. Ct. at 2714.

87. *See id.* at 2722.

88. *Id.* at 2723.

89. Holder v. Humanitarian Law Project, 130 S. Ct. 2705, 2724 (2010).

90. *See id*.

91. *Id.* at 2725. In the State Department's view, "it is highly likely that any material support to these organizations will ultimately inure to the benefit of their criminal, terrorist functions—regardless of whether such support was ostensibly intended to support non-violent, non-terrorist activities." *Id.* at 2727.

92. *See* Freedom of Information Act of 1966 § 1, 5 U.S.C § 552 (2012). The nine exemptions under the statute include records: (1) properly classified as secret in the interest of national defense or foreign policy, (2) related solely to internal personnel rules and practices, (3) specifically exempted by other statutes, (4) concerning trade secrets and commercial or financial information obtained from a person that is privileged or confidential, (5) privileged interagency or intra-agency memoranda or letters, except under certain circumstances (6) personnel, medical, and similar files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy, (7) investigatory records compiled for law enforcement purposes, (8) contained in or related to certain examination, operating, or condition reports concerning financial institutions, and (9) geological and geophysical information and data, including maps, concerning wells. *See id.* § 552(b). FOIA was amended in 1996 so that electronic requests for information could also be made. *See* Electronic Freedom of Information Act Amendments of 1996, Pub. L. No. 104-231, 110 Stat. 3048 (codified as amended at 5 U.S.C. § 552 (2012)).

legislative branch) nor the federal courts (the judicial branch) are subject to FOIA's provisions.[93] The purpose of FOIA is to grant public access to government information and to minimize administrative burdens.[94] Prior to FOIA's enactment, restrictive agency interpretations of government regulations were being used to withhold information from the public.[95] At a more local level, states have also followed the federal model by granting access to state government information through corresponding state statutes.[96]

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 regulates a specific category of information, notably individual health information.[97] HIPAA's implementing regulations create a complex set of privacy and security protections for individually identifiable health information maintained by covered entities and their business associates.[98] In addition, HIPAA provides patients with a variety of rights respecting their individual health information, including rights of access and inspection, accounting of disclosures, and restrictions on certain disclosures of health information to third parties.[99] Civil monetary penalties may also be imposed for failure to comply with HIPAA.[100]

The Fair and Accurate Credit Transaction Act (FACTA) of 2003 is designed to combat identity theft.[101] It allows consumers to get a free credit report from each of the three major consumer credit reporting agencies (Equifax, Experian, and TransUnion) every twelve months, and to place alerts on their credit histories under certain circumstances.[102] The law also sets standards for the masking, sharing, and disposal of sensitive financial data, such as credit card and Social Security numbers.[103]

93. *See* 5 U.S.C. § 551(1) (exempting Congress and U.S. courts from definition of agency).

94. *See* NLRB v. Robbins Tire & Rubber Co., 437 U.S. 214, 242 (1978) ("The basic purpose of FOIA is to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed.").

95. *See* EPA v. Mink, 410 U.S. 73, 79 (1973) (discussing legislative purpose of FOIA to increase disclosure), *superseded by statute*, Act of Nov. 21, 1974, Pub. L. No. 93-502, 88 Stat. 1561, *as recognized in* NLRB v. Robbins Tire & Rubber Co., 437 U.S. 214 (1978).

96. *See, e.g.*, CAL. GOV'T CODE §§ 6250-6258 (West 2013); MASS. GEN. LAWS ANN. ch. 66, § 10 (West 2013); N.Y. PUB. OFF. LAW §§ 84-90 (McKinney 2013).

97. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 262(a), 110 Stat. 1936, 2023 (codified as amended at 42 U.S.C. § 1320d-1 (2012)).

98. *See* 45 C.F.R. §§ 160.101-.552, 164.102-.534 (2013) (setting forth HIPAA privacy and security implementation rules).

99. *See id.* §§ 164.500-.534 (creating patient rights respecting protected health information). HIPAA grants patients the right to request that their records not be shared with third parties, but no authorization is necessary for one doctor's office to transfer a patient's medical records to another doctor's office for treatment purposes; similarly, a covered entity under the regulations is permitted to use or disclose protected health information without patient authorization for treatment, payment or health care operations. *See id.*

100. *See* 42 U.S.C. § 1320d-5 (2012) (establishing tiered penalty scheme).

101. *See* Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108–159, 117 Stat. 1952 (codified as amended in scattered sections of 15 and 20 U.S.C.).

102. *See* 15 U.S.C. § 1681j (2012).

103. *See id.* § 1681w.

Congress enacted the Wireless Communication and Public Safety Act of 1999 in response to the rise in wireless mobile device use.[104] The Act requires all mobile telephones created after the year 2000 to have the capability to map the user's location through the use of global positioning systems.[105] This permissible disclosure of caller location information without caller consent enables emergency services personnel to respond to calls much sooner.[106]

Finally, the First Amendment allows state tort law doctrine to compensate plaintiffs who claim injury arising out of misuse of information. In *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, Dun & Bradstreet, a credit reporting agency, paid damages for mistakenly reporting to some of its subscribers that the construction contractor Greenmoss Builders had voluntarily filed for bankruptcy.[107] The Court held that because the defamatory speech did not involve a public figure or a matter of public concern, the First Amendment places no limitations on the states in determining the level of compensation for the plaintiff's injuries.[108]

In *Zacchini v. Scripps-Howard Broadcasting Co.*, the plaintiff was an entertainer in a "human cannonball" act in which he was shot from a cannon into a net, and he was engaged to perform his act at an Ohio county fair.[109] A freelance reporter for Scripps-Howard Broadcasting Co. attended the fair and videotaped the plaintiff's entire act for a news program without the plaintiff's consent.[110] The Court held that Scripps-Howard's privileged free speech did not extend to broadcasting the plaintiff's entire performance without permission, noting the plaintiff's interest in the case was akin to a common-law copyright.[111]

In *Time, Inc. v. Hill*, Hill, his wife, and five children, involuntarily became the subjects of a front-page news story after being held hostage by three escaped convicts in their suburban home.[112] Years later, the defendant published a magazine article about the family despite the family's objection, which allegedly misrepresented Hill's former accounts of the hostage situation.[113] The Court overturned the jury's finding of liability for the

104. *See* Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106–81, § 2, 113 Stat. 1286, 1286-87.

105. *See* 47 U.S.C. § 222 (2012) (permitting sharing of caller information in circumstances without caller permission).

106. *See id.*

107. *See* 472 U.S. 749, 763 (1985) (recovering damages in defamation cases absent showing of malice does not violate First Amendment).

108. *See id.*

109. *See* 433 U.S. 562, 563 (1977).

110. *See id.* at 563-64.

111. *See id.* at 578-79 ("[A]lthough the State of Ohio may as a matter of its own law privilege the press in the circumstances of this case, the First and Fourteenth Amendments do not require it to do so.").

112. *See* 385 U.S. 374, 378 (1967).

113. *See id.* at 378-79.

magazine, holding that absent malicious intent, the misleading article was still protected under the First Amendment.[114]

Hill and *Zacchini* illustrate the Court's divergent treatment of the press regarding the speech privileges afforded under the First Amendment. Some would suggest that the Court has afforded insufficient protection to the press, also referred to as the "Fourth Estate," despite its specific reference in the First Amendment.[115] Indeed, press complaints against government bars to accessing information have rarely been successful in claims for prison access, though claims for access to courtrooms and court records have fared better.[116] Additionally, journalists' claims for nondisclosure of confidential sources as essential to a vigorous press have never achieved First Amendment status, although various state statutes afford some protection.[117]

D. Recent Developments

Recent disclosures attributed to Edward Snowden, a twenty-nine-year-old former NSA contractor, describe a process for obtaining and enforcing warrants under the Foreign Intelligence Surveillance Act (FISA).[118] FISA warrant applications and the warrants themselves are secret, and the recipients are prohibited from disclosing the receipt of a warrant.[119] Thousands of FISA warrants have been served with this extraordinary enforced silence on each recipient.[120] Notwithstanding this high level of secrecy, the recipients of these

114. *See id.* at 387-88.

> We hold that the constitutional protections for speech and press preclude the application of the New York statute to redress false reports or matters of public interest in the absence of proof that the defendant published the report with knowledge of its falsity or in reckless disregard of the truth.

Id.

115. *See* Potter Stewart, *"Or of the Press"*, 26 HASTINGS L.J. 631, 633 (1975) (describing press as an outside check on government); *see also* U.S. CONST. amend I ("Congress shall make no law . . . abridging the freedom of speech, *or of the press*." (emphasis added)).

116. *See* Houchins v. KQED, Inc., 438 U.S. 1, 14 (1978) (rejecting argument for constitutional right of press access concerning conditions of jails); Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 580-81 (1980) (holding, absent overriding interest, right of press to attend criminal trials protected under First Amendment).

117. *See* Branzburg v. Hayes, 408 U.S. 665, 687, 689 (1972) (stating newsmen not exempt from duty to appear before grand jury and observing privileges under state laws).

118. *See* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 50 U.S.C.) (prescribing procedures for surveillance information); Glenn Greenwald et al., *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN, June 9, 2013, http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (describing context of Snowden disclosures).

119. *See* 50 U.S.C. § 1805 (2012) (describing requirements for issuance of FISA warrant).

120. *See* Letter from Reggie B. Walton, Presiding Judge, U.S. Foreign Intelligence Surveillance Court, to Charles E. Grassley, Ranking Member, Comm. on the Judiciary, U.S. Senate (Oct. 11, 2013) (describing frequency with which FISA warrant applications modified and granted), *available at* http://www.uscourts.gov/uscourts/courts/fisc/ranking-member-grassley-letter-131011.pdf.

warrants, often chief executives of communications or Internet companies, have a fiduciary duty to consult with lawyers and other experts about the implications of such data seizures and the Fourth Amendment rights of persons whose information is sought by the warrants.[121]

Edward Snowden's disclosures amount to one of the most significant leaks of sensitive domestic and foreign surveillance information in U.S. political history.[122] A one-page criminal complaint, filed in the United States District Court for the Eastern District of Virginia, accused Mr. Snowden of theft of government property and willful communication of classified communications intelligence to an unauthorized person.[123] In another recent noteworthy case, United States Army Private First Class/intelligence analyst Chelsea Manning (formerly Bradley Manning) was found guilty of espionage and stealing government property.[124]

Moving away from improper disclosure of sensitive government information to forms of electronic information, two controversies concerning "net neutrality" and Google books continue to garner attention. Net neutrality is the idea that all Internet content is treated similarly and travels at the same speed over the network, therefore, internet service providers cannot discriminate.[125] "This is the simple but brilliant 'end-to-end' design of the Internet that has made it such a powerful force for economic and social good . . . ."[126] Verizon is challenging network neutrality regulations promulgated by the FCC in the Court of Appeals for the D.C. Circuit. Verizon claims that the FCC rule prohibiting Verizon, as an internet service provider, from charging either the content provider or the customer a fee for internet access violates rights under the First and Fifth Amendments.[127]

In the Google books case, pending in the Second Circuit, The Authors Guild—a writers' interests advocacy group—is appealing a decision by a district court to dismiss its copyright suit.[128] The Guild continues to take the position that Google is not making "fair use" of copyrighted material by offering snippets of author's works. Google has defended its library, saying it is fully compliant with copyright law.

121. *See id.*

122. *See* Greenwald et al., *supra* note 118 (acknowledging gravity of Snowden disclosures).

123. *See* Complaint at 1, United States v. Snowden, No. 1:13 CR 265-CMH (E.D. Va. June 14, 2013).

124. *See* Erin Banco, *Judge Upholds Charge Against Manning*, N.Y. TIMES, July 18, 2013, http://www.nytimes.com/2013/07/19/us/judge-in-manning-case-allows-charge-of-aiding-the-enemy.html.

125. *See* Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J. TELECOMM. & HIGH TECH L. 141, 167-68 (2003) (explaining concept of network neutrality).

126. Lawrence Lessig & Robert W. McChesney, *No Tolls on the Internet*, WASH. POST, June 8, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/06/07/AR2006060702108.html.

127. *See* Joint Brief for Verizon and MetroPCS at 42-49, Verizon v. FCC, No. 11-1355 (D.C. Cir. July 2, 2012) (setting forth constitutional arguments against FCC regulations).

128. *See* Authors Guild Notice of Civil Appeal at 1, Authors Guild v. Google, Inc., No. 13-4829 (2d Cir. Dec. 23, 2013).

E. Summary

The Court in *Sorrell* recognizes a First Amendment right of access to information.[129] There is no soapbox, no advocacy. A physician writes a prescription for a specific patient in the privacy of her office. The doctor is the speaker and the druggist is the listener, who is obligated by statute to enter the information into an electronic database. The information is transmitted electronically to the State, which has hired a database consultant who develops software that will serve the purposes of Act 80. The database exists in response to governmental demand. Once amassed, however, the data has economic value to a data miner who now claims a right of access. The Court held that the First Amendment polices the line between the data seeker and the data creator, and now holder.[130] The result favors access because the Court views skeptically restrictions on factual information found to be speech.[131] In *Reed*, the plea by initiative supporters for the secrecy of their political advocacy, lest it be chilled in the future, fails in favor of a right to access data.[132] In *McIntyre*, the Court found a ban on speaking anonymously in campaigns would improperly reduce speakers and points of view.[133]

Trans Union and *U.S. West, Inc.* each involve federal restrictions, one statutory and the other administrative, on the use and dissemination of data created for an internal business reason.[134] The creators and holders of the data object to the government's limitation on the uses of the data. Again, the data is speech, and its economic value is destroyed by the restrictions. Courts invalidate these restrictions under the rubric of freer movement of information under the First Amendment. The court in *Glik* protects the act of gathering

129. *See* Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2659 (2011).

130. *See id.* at 2663 (finding Vermont law exacts speech restrictions on recipient speakers); *see also* Ashutosh Bhagwat, Sorrell v. IMS Health*: Details, Detailing, and the Death of Privacy*, 36 VT. L. REV. 855, 880 (2012) (arguing *Sorrell* constitutes an unwarranted expansion of First Amendment doctrine).

131. Justice Breyer argued in his dissenting opinion that Vermont was making an acceptable legislative decision to try to reduce medical costs and encourage the use of generics similar to those involved in *Glickman v. Wileman Brothers & Elliott, Inc.*, 521 U.S. 457 (1997), in which the Court considered the First Amendment's application to federal agricultural commodity marketing regulations requiring fruit growers to make compulsory contributions to pay for collective advertising. *See Sorrell*, 131 S. Ct. at 2673 (Breyer, J., dissenting); *Glickman,* 521 U.S. at 460-61. In *Glickman,* the Court reviewed the lawfulness of the regulation's negative impact on the growers' freedom voluntarily to choose their own commercial messages "under the standard appropriate for the review of economic regulation." *Glickman*, 521 U.S. at 469; *see* Johanns v. Livestock Mktg. Ass'n., 544 U.S. 550, 560-62 (2005) (applying less scrutiny when compelled speech made by Government); United States v. United Foods, Inc., 533 U.S. 405, 412 (2001) (applying greater scrutiny where compelled speech "principal object" of regulatory scheme).

132. Doe v. Reed, 130 S. Ct. 2811, 2822 (2010) (holding First Amendment not violated by disclosure of referendum petitions).

133. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 334 (1995) (holding prohibition of distribution abridges freedom of speech).

134. *See* Trans Union Corp. v. FTC, 245 F.3d 809, 811 (D.C. Cir. 2001) (restricting sales of credit reports); U.S. West, Inc. v. FCC, 182 F.3d 1224, 1228-29 (10th Cir. 1999) (restricting use of customer proprietary information).

information by cell phone video and ties it to citizen empowerment to check the agents of an overreaching government.[135] The *Bartnicki* and *New York Times* cases favor the publication of accurate information about how government operates behind closed doors even when the source of the information was a criminal act.[136]

The exception to unburdened speech always seems to involve matters of national security, which is perhaps caused by the Supreme Court's self-doubt about the propriety of its institutional role in interfering with Congress and the Commander-in-Chief. The conviction of Abrams for leafleting against World War I and of Dennis for organizing the Communist Party could have been viewed as expanding the pie of political information in the marketplace of ideas, but the Court rejected that characterization and allowed these types of speech at these moments in history to be punished. The Humanitarian Law Project's courses on mediation and alternative dispute resolution could likewise have been viewed as acts of spreading knowledge and expertise, but instead the Court deferred to Congress and the State Department.[137] Certainly the disclosures of Edward Snowden have informed the American public of the Internet's vulnerability. But perhaps it is naïve to believe that the Court should be immune to the hysteria surrounding wars, communism, and terrorism.

Certainly, FOIA has accelerated the access of data miners, researchers, and curious intermeddlers to a treasure trove of information held by the executive branch. Further, the statutory organization and regulation of the national credit reporting system and individual medical records through HIPPA have facilitated the exchange of private information combined with attempts to limit access to private information.

Tort judgments, which restrict data, do not undermine the trend toward access. *Hill* and *Zacchini* seem to be less about the free flow of information and more about the individual rights of the plaintiff crime victims—Hill objected to being subjected to publicity, and Zacchini's carnival act lost spectators because of the evening news.[138] Finally, Greenmoss suffered economic loss from a negligent data manager.[139]

135. *See* Glik v. Cunniffe, 655 F.3d 78, 82 (1st Cir. 2011) (recording public officials acting in their official capacity permissible).

136. *See* Bartnicki v. Vopper, 532 U.S. 514, 517 (2001) (intercepting cell phone conversation by unlawful means); N.Y. Times Co. v. United States, 403 U.S. 713, 714 (1971) (per curiam) (permitting publication of classified historical study).

137. *See* Holder v. Humanitarian Law Project, 130 S. Ct. 2705, 2731 (2010) (upholding statutory prohibition on funding designated foreign terrorist organizations).

138. *See* Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 562, 575 (1977) (noting carnival act lost spectators to evening news); Time, Inc. v. Hill, 385 U.S. 374, 378 (1967) (noting objections to publicity following misrepresentations about former hostage situation).

139. *See* Dun & Bradstreet, Inc. v. Greemoss Builders, Inc., 472 U.S. 749, 751-52 (1975).

III. FOURTH AMENDMENT LIMITATIONS ON ACCESS TO DATA

The framers of the Constitution could not have predicted the complexities of today's technology—access to information was severely limited at that time, and communication was only as fast as a horse or a transatlantic ship. Nonetheless, early Supreme Court cases and constitutional doctrine illustrate not only a concern about intrusions into one's personal predilections, but also a fear that eavesdropping will compromise conversations of innocent third parties. Ultimately, Fourth Amendment limitations on data access reflect the fundamental skepticism that government will abuse its granted powers.

A. History

The Fourth Amendment to the U.S. Constitution protects the security of one's person, house, papers and effects against unreasonable searches and seizures.[140] Before our separation from England, writs of assistance authorized customs agents representing the King of England to search homes for smuggled goods.[141] The colonists were well aware of the English case, *Entick vs. Carrington*, wherein royal representatives broke into the private home of John Entick in search of material that was critical of the King and his policies.[142] In the process, they broke into locked boxes and desks, and confiscated many papers, charts, and pamphlets. Entick charged that the entire search and seizure had been unlawfully conducted, and the court agreed.[143] The court said that the Crown had no power to issue such orders, there was no demonstration of probable cause that a crime had been committed, and the warrant was too broad because it allowed a general confiscation of anything the officers found.[144]

In *Boyd v. United States*,[145] the Court invalidated a customs enforcement act, which required a defendant charged with smuggling to produce his business books as part of his defense against the charges.[146] The Court invalidated the statute stating,

> [b]reaking into a house and opening boxes and drawers are circumstances of aggravation; but any forcible and compulsory extortion of a man's own testimony, or of his private papers to be used as evidence to convict him of crime, or to forfeit his goods, is within the condemnation of that judgment. In

140. U.S. CONST. amend IV.

141. *See* Tracey Maclin, *The Complexity of the Fourth Amendment: A Historical Review*, 77 B.U. L. REV. 925, 945 (1997) (describing use of writs of assistance).

142. *See* (1765) 95 Eng. Rep. 807 (K.B.) 807-08.

143. *See id.* at 808, 817.

144. *See id.* at 817-18.

145. 116 U.S. 616 (1886).

146. *See* Act of June 22, 1874, ch. 391, § 5, 18 Stat. 186, 187, *invalidated by* Boyd v. United States, 116 U.S. 616 (1886).

this regard the fourth and fifth amendments run almost into each other.[147]

In 1890, Samuel D. Warren and future Supreme Court Justice Louis D. Brandeis published their influential article, *The Right of Privacy*, which complained that "[i]nstantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[148] Later, in 1928, Justice Brandeis dissented in *Olmstead* wherein a majority of the Court held that evidence coming from a wiretap without a warrant was admissible against a defendant charged with bootlegging.[149] He summarized the purposes of the Fourth and Fifth Amendments:

> When the Fourth and Fifth Amendments were adopted, "the form that evil had theretofore taken" had been necessarily simple. Force and violence were then the only means known to man by which a government could directly effect self-incrimination. It could compel the individual to testify—a compulsion effected, if need be, by torture. It could secure possession of his papers and other articles incident to his private life—a seizure effected, if need be, by breaking and entry. Protection against such invasion of "the sanctities of a man's home and the privacies of life" was provided in the Fourth and Fifth Amendments by specific language. But "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.[150]

147. *Boyd*, 116 U.S. at 630.

148. Samuel D. Warren & Louis D. Brandeis, *The Right of Privacy*, 4 HARV. L. REV. 193, 195 (1890).

> The right of one who has remained a private individual, to prevent his public portraiture, presents the simplest case for such extension; the right to protect one's self from pen portraiture, from a discussion by the press of one's private affairs, would be a more important and far-reaching one. If casual and unimportant statements in a letter, if handiwork, however inartistic and valueless, if possessions of all sorts are protected not only against reproduction, but against description and enumeration, how much more should the acts and sayings of a man in his social and domestic relations be guarded from ruthless publicity. If you may not reproduce a woman's face photographically without her consent, how much less should be tolerated the reproduction of her face, her form, and her actions, by graphic descriptions colored to suit a gross and depraved imagination.

Id. at 213-14.

149. *See* Olmstead v. United States, 277 U.S. 438, 464 (1928), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

150. *Id.* at 473 (Brandeis, J., dissenting) (citation omitted).

Additionally, Justice Brandeis predicted that "[t]he progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping."[151] He further summarized,

> The evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails. Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard. . . . As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire tapping.[152]

In *Katz v. United States*, the Court overturned *Olmstead* and held that wiretaps, even of public telephone booths, were unconstitutional searches because there was a reasonable expectation that the communication would be private.[153] Much of the Court's reasoning in *Katz* is derived from the Brandeis dissent in *Olmstead*:

> The Government stresses the fact that the telephone booth from which the petitioner made his calls was constructed partly of glass, so that he was as visible after he entered it as he would have been if he had remained outside. But what he sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen. No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.[154]

151. *Id.* at 474 (Brandeis, J., dissenting).

152. *Id.* at 475-76 (Brandeis, J., dissenting).

153. *See* Katz v. United States, 389 U.S. 347, 353 (1967). *See generally* Mary Graw Leary, Katz *on a Hot Tin Roof—Saving the Fourth Amendment from Commercial Conditioning by Reviving Voluntariness in Disclosures to Third Parties*, 50 AM. CRIM. L. REV. 341 (2013) (exploring possible judicial responses to eroding privacy expectations).

154. *Katz*, 389 U.S. at 352 (footnotes omitted).

B. Newer Technologies

In *Kyllo v. United States*, the Court applied the expectation of privacy test to heat monitors.[155] Federal agents used a heat monitor to scan the exterior of a home in order to detect whether it was being used to grow marijuana.[156] The Court held that use of the thermal-imaging technology, which is not generally available for public use, to obtain information regarding the interior of the home was an unlawful search without a proper warrant.[157] The Court acknowledged that a mechanical interpretation of the Fourth Amendment was rejected in *Katz* where "the eavesdropping device picked up only sound waves that reached the exterior of the phone booth."[158] The Court further acknowledged that "[w]hile the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development."[159]

In *Florida v. Jardines*, the Court "consider[ed] whether using a drug-sniffing dog on a homeowner's porch to investigate the contents of the home is a 'search' within the meaning of the Fourth Amendment."[160] After receiving an unverified tip that marijuana was being grown in the home of the defendant, the police approached Jardines' home accompanied by a drug-sniffing dog.[161] As the dog approached Jardines' front porch, he began energetically exploring the area for the strongest point source of that odor.[162] On the basis of the dog's reaction, the police obtained a warrant to search the residence.[163] The search revealed marijuana plants and the defendant was charged with trafficking in cannabis, however, the evidence was suppressed at trial.[164] The Court affirmed the suppression because the intrusion of the trained dog on to the premises of the defendant's home violated the Fourth Amendment.[165] At the Fourth

155. *See* 533 U.S. 27, 33-35 (2001).
156. *See id*. at 29.
157. *See id*. at 40.
158. *Id.* at 35.
159. *Kyllo*, 533 U.S. at 36.
160. *See* 133 S. Ct. 1409, 1413 (2013).
161. *See id.* at 1413.
162. *Id.*
163. *Id.*
164. *Jardines*, 133 S. Ct. at 1413.
165. *See id.* at 1417 (holding use of drug-sniffing dog on porch constituted trespass of curtilage). However, in *Illinois v. Caballes*, the Supreme Court ruled that police do not need reasonable suspicion to use drug dogs to sniff a vehicle during a legitimate traffic stop. *See* 543 U.S. 405, 410 (2005). In *Caballes*, the defendant was pulled over for speeding and subsequently arrested for marijuana trafficking after a drug dog alerted to his vehicle when brought to the scene by a second officer. The Illinois Supreme Court reversed Caballes' conviction, holding that a drug sniff was unreasonable without evidence of a crime other than speeding. However, in a six-to-two ruling, the Supreme Court held that the Fourth Amendment is not implicated when police use a dog sniff during the course of a legal traffic stop. Justice Stevens wrote the opinion of the Court, reasoning that because dog sniffs only identify the presence of illegal items in which citizens have no legitimate privacy interests, the Fourth Amendment does not apply to the use of drug dogs. *See Caballes*, 543 U.S. at 409. As a result, *Caballes* authorizes police to walk a drug dog around a vehicle

Amendment's "'very core' stands 'the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'"[166] The Court reasoned that this right and the right to retreat would be significantly diminished if the "State's agents could stand in a home's porch or side garden and trawl for evidence with impunity. . . [or] observe [one's behavior] from just outside the front window."[167]

In *United States v. Jones*, the Court decided the government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constituted a search.[168] In an opinion authored by Justice Scalia, the Court emphasized that "[t]he Government had physically occupied private property for the purpose of obtaining information" on the defendant's whereabouts, and the framers of the Constitution likely anticipated such occupation to constitute a search under the Fourth Amendment.[169]

The Court also pointed out the historical connection between the concept of a search and property, noting, "Fourth Amendment jurisprudence was [originally] tied to common-law trespass . . . ."[170] In later cases, the Court has deviated from the exclusively property-based approach. For example, in *Katz*, the Court stated that "the Fourth Amendment protects people, not places," and recognized a violation in the attachment of an eavesdropping device to a public telephone booth because there was a "reasonable expectation of privacy."[171] Today, the Court uses both the reasonable expectation of privacy concept and common-law notions of trespass when analyzing the constitutionality of surveillance practices under the Fourth Amendment.[172]

In *Missouri v. McNeely*, the police perceived the defendant as showing signs

during any legitimate traffic stop. If the dog signals that it smells drugs, police then have probable cause to conduct a search. However, the ruling does not allow police to detain the suspect indefinitely until dogs arrive. The legitimacy of the traffic stop still depends on its duration—if police cannot bring a dog to the scene in the time it takes to run a motorist's tags and write a ticket, the use of the dog becomes constitutionally suspect.

166. Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013) (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

167. *Id.*

168. *See* 132 S. Ct. 945, 949 (2012).

169. *Id.*; *see* Boyd v. United States, 116 U.S. 616, 626 (1886) (acknowledging American statesmen's awareness of freedom with regard to searches and seizures); Entick v. Carrington, (1765) 95 Eng. Rep. 807 (K.B.).

> [O]ur law holds the property of every man so sacred, that no man can set his foot upon his neighbour's close without his leave; if he does he is a trespasser, though he does no damage at all; if he will tread upon his neighbour's ground, he must justify it by law.

Entick, 95 Eng. Rep. at 817

170. *Jones*, 132 S. Ct. at 949.

171. Katz v. United States, 389 U.S. 347, 351 (1967); *see* David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381, 385-59 (2013) (describing influence of new technologies on concept of surveillance).

172. *See Jones*, 132 S. Ct. at 953 (explaining reasonable expectation of privacy concept under *Katz* not exclusive test).

of intoxication, including bloodshot eyes, slurred speech, and the smell of alcohol on his person.[173] McNeely performed multiple field-sobriety tests poorly, was arrested, and subsequently taken to the local hospital for a blood test without a search warrant.[174] At trial, McNeely moved to suppress the results of the blood test.[175] In analyzing whether there is an exception to the Fourth Amendment warrant requirement for forcibly drawing blood from a person suspected of drunk driving, the Court looked to *Schmerber v. California*.[176] In *Schmerber*, the "Court upheld a warrantless blood test of an individual arrested for driving under the influence of alcohol because the officer 'might reasonably have believed that he was confronted with an emergency, in which the delay necessary to obtain a warrant, . . . threatened the destruction of evidence."[177] In *McNeely*, the Court was reluctant to create a bright-line rule, holding that natural blood metabolism does not create a per se exigency justifying an exception under the Fourth Amendment; instead exigency must be determined case-by-case based on the totality of the circumstances.[178] The State failed to present evidence of exigency, and therefore, the Court upheld the suppression of the warrantless blood test.[179]

However, the Court refused to suppress evidence obtained from technologies in *Smith v. Maryland*[180] and *Maryland v. King*.[181] In *Smith*, the Court declined to extend an expectation of privacy to the installation of a pen register on the defendant's phone line at the telephone company because the information captured by the pen register was no different than information recorded by the telephone company for billing purposes.[182] In *King*, the Court addressed Maryland's DNA Collection Act, which authorizes law enforcement officers to collect DNA samples from a person who is arrested for, but not yet convicted of, violent crimes or burglary.[183] Police arrested King in 2009 on assault

173. *See* 133 S. Ct. 1552, 1556-57 (2013).

174. *See id.*

175. *See id.* at 1557.

176. *See id.* at 1556 (citing Schmerber v. California, 384 U.S. 757 (1966)).

177. *McNeely*, 133 S. Ct. at 1556 (quoting *Schmerber*, 384 U.S. at 770)).

178. *See id.* at 1563 ("[W]hile the natural dissipation of alcohol in the blood may support a finding of exigency in a specific case, as it did in *Schmerber*, it does not do so categorically.").

179. *See* Missouri v. McNeely, 133 S. Ct. 1552, 1567-68 (2013).

180. 442 U.S. 735 (1979).

181. 133 S. Ct. 1958 (2013).

182. *See Smith*, 442 U.S. at 745-46. The Court held that a pen register—a device that records and stores the numbers called from a particular phone—installed at the telephone company's central offices at the request of the police is not a search because the "petitioner voluntarily conveyed numerical information to the telephone company." *Id.* at 744. Because the defendant had disclosed the dialed numbers to the telephone company in order to connect his call, he did not have a reasonable expectation of privacy in the numbers he dialed. *See id.* The Court rejected the idea that the installation and use of a pen registry constitutes a violation of one's legitimate expectation of privacy because the numbers would be available to and recorded by the phone company anyway. *See id.* at 745. The Court did not distinguish between disclosing the numbers to a human operator or simply to the automatic equipment used by the telephone company. *See id.*

183. *See King*, 133 S. Ct. at 1966.

charges, and on the day of his arrest, personnel at the booking facility swabbed King's mouth to collect his DNA sample and sent it off for processing.[184] King's DNA record was uploaded to Maryland's DNA database, and was matched to a DNA sample collected in an unrelated, unsolved 2003 rape case. King was later charged with the 2003 rape and sought suppression of the DNA identification due to the manner of the collection and its subjection to an extensive bureaucratic process.[185] The Court upheld the collection and the process, reasoning that "[t]he routine administrative procedure[s] at a police station house incident to booking and jailing the suspect" further a variety of legitimate interests.[186]

Further, the Court observed that "[a] suspect's criminal history is a critical part of his identity that officers should know when processing him for detention," and in this respect, DNA analysis and fingerprint databases are similar.[187] The Court also noted, "in the interests of justice, the identification of an arrestee as the perpetrator of [another] heinous crime may have the salutary effect of freeing a person wrongfully imprisoned for the same offense."[188]

The Court also rejected a claim that use of the FBI-sponsored Combined DNA Index System (CODIS) was a violation of the Fourth Amendment.[189] While science can always progress further, and those progressions may have Fourth Amendment consequences, CODIS loci "are not at present revealing information beyond identification."[190] The argument that the collection in *King* "reveals any private medical information at all is open to dispute . . . . [However], the [law] provides statutory protections that guard against further

184. *See id.*

185. *See id*; *see also* Dist. Attorney's Office v. Osborne, 557 U.S. 52, 55 (2009) (observing DNA's ability to both exonerate wrongly convicted and to identify guilty); Erin Murphy, *Databases, Doctrine & Constitutional Criminal Procedure*, 37 FORDHAM URB. L. J. 803, 833 (2010) (suggesting constitutional inquiry ends when collection of DNA samples permissible); Erin Murphy, *DNA and the Fifth Amendment* 3 (N.Y.U. Sch. of Law Pub. Law & Legal Theory Research Paper Series, Working Paper No. 11-28, May 2011), *available at* http://ssrn.com/abstract=1823722 (showing several states have mandatory DNA sampling procedures).

186. *King*, 133 S. Ct. at 1971 (alteration in original) (quoting Illinois v. Lafayette, 462 U.S. 213, 238 (1983)) (internal quotation marks omitted).

187. Maryland v. King, 133 S. Ct. 1958, 1971-72 (2013). "By comparison to this substantial government interest and the unique effectiveness of DNA identification, the intrusion of a cheek swab to obtain a DNA sample is a minimal one." *Id.* at 1977.

188. *Id.* at 1974; *see* Joseph Goldstein, *Police Agencies Are Assembling Records of DNA*, N.Y. TIMES, June 12, 2013, http://www.nytimes.com/2013/06/13/us/police-agencies-are-assembling-records-of-dna.html (describing variations in policies regarding arrestee DNA collection).

189. *See King*, 133 S. Ct. at 1979. CODIS and the National DNA Index System (NDIS) are used in law enforcement crime laboratories to foster the exchange and comparison of forensic DNA evidence from violent crime investigations. *See Laboratory Services: Combined DNA Index System (CODIS)*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/lab/biometric-analysis/codis (last visited Mar. 12, 2014).

190. *King*, 133 S. Ct. at 1979 (quoting Sarah. H. Katsanis & Jennifer K. Wagner, *Characterization of the Standard and Recommended CODIS Markers*, 58 J. FORENSIC SCI. S169, S171 (2013)).

invasion of privacy."[191]

C. National Security Cases

Since the founding of the Republic, American presidents have felt a special duty to keep the country safe when facing foreign countries with uncertain intentions. Those intentions could be culled through legitimate means of diplomacy, or through more unseemly methods like spying or interference with communications. For instance, in 1862 President Abraham Lincoln approved a request by Secretary of War Edwin M. Stanton that included total control of the telegraph lines by rerouting those lines through his office.[192] During the Cold War, both the Soviet Union and the United States sent spy planes over each other's territory to gain intelligence information.[193]

In 1978, through its enactment of FISA, Congress authorized the government to monitor private electronic communications between the United States and a foreign country if the government's purpose was primarily to obtain foreign intelligence information, the surveillance target was a foreign power or an agent of a foreign power, and the surveillance procedures used were designed to minimize the acquisition, retention, and dissemination of private information acquired about Americans.[194] In order to conduct any such surveillance, the requesting party had to obtain the approval of the Foreign

191. *Id.* at 1979.

192. *See* David T. Z. Mindich, *Lincoln's Surveillance State*, Op-Ed., N.Y. TIMES, July 5, 2013, http://www.nytimes.com/2013/07/06/opinion/lincolns-surveillance-state.html (describing Stanton's intent by rerouting phone lines).

193. *See This Day in History, May 1, 1960: American U-2 Spy Plane Shot Down*, HISTORY, http://www.history.com/this-day-in-history/american-u-2-spy-plane-shot-down (last visited Mar. 12, 2014).

> An American U-2 spy plane [was] shot down while conducting espionage over the Soviet Union. The incident derailed an important summit meeting between President Dwight D. Eisenhower and Soviet leader Nikita Khrushchev that was scheduled for later that month.
>
> The U-2 spy plane was the brainchild of the [CIA] . . . . [The plane could] take high-resolution pictures of headlines in Russian newspapers as it flew overhead. Flights over the Soviet Union [for espionage purposes] began in mid-1956.
>
> On May 1, 1960, a U-2 flight . . . disappeared while on a flight over Russia. The CIA reassured the president that, even if the plane had been shot down, it was equipped with self-destruct mechanisms that would render any wreckage unrecognizable and the pilot was instructed to kill himself in such a situation. Based on this information, the U.S. government issued a cover statement indicating that a weather plane had veered off course and supposedly crashed somewhere in the Soviet Union. With no small degree of pleasure, Khrushchev pulled off one of the most dramatic moments of the Cold War by producing not only the mostly-intact wreckage of the U-2, but also the captured pilot—very much alive. A chagrined Eisenhower had to publicly admit that it was a U.S. spy plane.

Id.

194. *See* 50 U.S.C. §§ 1801(e), (h) (2012) (defining electronic surveillance and minimization procedures).

Intelligence Surveillance Court (FISC), which was also created by the Act.[195] An application to the FISC needs to describe each target, the nature of the information sought, and the communications or activities to be subjected to the surveillance.[196] The application must also certify that, in significant part, it seeks to obtain foreign intelligence information; it must demonstrate probable cause to believe that each specified target is a foreign power or an agent of a foreign power; and it needs to describe the procedures to be used to minimize intrusions upon Americans' privacy.[197] The FISC convenes in secret and hears applications presented by the Justice Department, and its orders and decisions are similarly confidential.[198] Investigative journalists are the public's only source of information about the court.[199]

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), the chief response to the terrorist attacks of September 11th, expanded and strengthened the government's ability to gather intelligence within the United States. The USA PATRIOT Act, among other things, expanded the Secretary of the Treasury's authority to regulate financial transactions, particularly those involving foreign individuals and entities, and broadened the powers of law enforcement and immigration authorities in detaining and deporting immigrants suspected of terrorism-related acts.[200]

195. *See id.* § 1803(a)(1).

> The Chief Justice of the United States shall publicly designate 11 district court judges from at least seven of the United States judicial circuits of whom no fewer than 3 shall reside within 20 miles of the District of Columbia who shall constitute a court which shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this chapter . . . .

Id.

196. *See id.* § 1804(a).

197. *See id.* §§ 1804(a), 1805(d)(3).

198. *See* 50 U.S.C. § 1802 (describing FISC applications under seal). *But see* James G. Carr, Op-Ed., *A Better Secret Court*, N.Y. TIMES, July 22, 2013, http://www.nytimes.com/2013/07/23/opinion/a-better-secret-court.html (proposing appointment of lawyers to represent public interest in some warrant application proceedings).

199. *See* Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N.Y. TIMES, July 6, 2013, http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html?pagewanted=all (explaining secret body of law developed in FISC). Justices sitting on the FISC acknowledge the majority of surveillance applications submitted to the court have been approved, including nearly 1800 applications submitted in 2012. *See id.* As a justification for FISA surveillance orders, the Justice Department often relies on the FISC's use of a Supreme Court principle called the "special needs doctrine," which the FISC has used to "carve[] out an exception to the Fourth Amendment's requirement of a warrant for searches and seizures." *Id.* For example, in one recent case, intelligence officials obtained access to e-mails sent within the United States, which allegedly contained schematic drawings and diagrams connected to Iran's nuclear program. *See id.* Normally, a court warrant would be required, however, the expended reach of the FISA rules enabled such access. *See id.*

200. *See generally* USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of U.S.C.) (enhancing domestic security and surveillance measures).

Congress further extended the reach of the government's surveillance programs when it enacted the FISA Amendments Act in 2008, setting forth three significant changes.[201] First, it eliminated the requirement that the government describe to the FISC each specific target and identify each facility at which its surveillance would be directed, thus permitting surveillance on a programmatic, but not necessarily individualized, basis.[202] Second, it permitted the Attorney General and Director of National Intelligence to jointly authorize surveillance of persons outside the United States for one-year periods.[203] Third, it diminished the court's authority to insist upon, and eliminated its authority to supervise, instance-specific procedures to minimize privacy intrusion, though court-approved general minimization procedures must still be used.[204] As a result of these changes, the government can obtain approval for its surveillance of electronic communications within and between the United States and targets in foreign territories by showing the court "a significant purpose of the acquisition is to obtain foreign intelligence information," and it will use general targeting and privacy-intrusion minimization procedures of a kind the court had previously approved.[205]

In the summer of 2013, a series of newspaper articles described the extent to which the U.S. government had been using powers enacted by the FISA Amendments Act of 2008. The NSA and the FBI were reported to be "tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets."[206] Using the

201. FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (codified in scattered sections of 50 U.S.C.).

202. *See* 50 U.S.C. § 1881a(g)(4) (2012).

203. *See id.* § 1881a(a).

204. *See id.* § 1881a(e).

205. *See id.* § 1881a(e), (g)(2)(A)(v). Conventional U.S. courts (i.e., non-FISCs) have also reviewed instances of search and surveillance of persons located outside the United States. *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 261 (1990) (reviewing validity of search conducted at individual's residence in Mexico). Verdugo-Urquidez, an alleged drug kingpin operating wholly out of Mexico, imported a network of drugs into the United States. *See id.* at 262. Following an arrest by the Mexican police, U.S. Drug Enforcement Agency officers searched the defendant's home and seized evidence. *See id.* The Court held there is no extraterritorial reach under the Fourth Amendment. *See id.* at 274-75

> Some who violate our laws may live outside our boarders under a regime quite different from that which obtains in this country. Situations threatening to important American interests may arise half-way around the globe, situations which in the view of the political branches of our Government require an American response with armed force. If there are to be restrictions on searches and seizures which occur incident to such American action, they must be imposed by the political branches through diplomatic understanding, treaty, or legislation.

Id. at 275.

206. Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST, June 7, 2013, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da

secret program named Prism, these agencies ordered Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple, in exchange for immunity from lawsuits, to open their servers to the FBI's Data Intercept Technology Unit, which is responsible for liaisons between the U.S. companies and the NSA.[207]

Reports also surfaced in 2013 that the "Obama administration [was] secretly carrying out a domestic surveillance program under which it [was] collecting business communication records involving Americans . . . according to a highly classified court order . . . ."[208] Signed by FISC Judge Roger Vinson, this order directed a Verizon subsidiary "to turn over 'on an ongoing daily basis' to the [NSA] all call logs 'between the United States and abroad' or 'wholly within the United States, including local telephone calls.'"[209] "The order [did] not apply to the content of the communications," and it prohibited the recipients of the order from discussing its existence.[210]

Not all of the businesses subject to the FISA order initially complied. In fact, Yahoo tried to refuse compliance, "saying the broad requests were unconstitutional."[211] The judges rejected Yahoo's argument, leaving them with two choices: either comply with the order and provide the data or break the law.[212] Faced with these options, Yahoo became part of the NSA's secret Internet surveillance program along with the other named companies.[213]

In *Clapper v. Amnesty International USA*, the plaintiffs, American-based human rights groups with a focus on foreign countries, launched an anticipatory legal attack on the 2008 FISA amendments.[214] The plaintiffs feared their communications were being wiretapped in violation of their Fourth Amendment rights.[215] The Court affirmed dismissal of the complaint,

8-cebf-11e2-8845-d970ccb04497_story.html (reporting on wiretapping activities by NSA and FBI).

207. *See id.*; *see also* John Shiffman & Kristina Cooke, *DEA Special Operations Division Covers up Surveillance Used To Investigate Americans: Report*, HUFFINGTON POST (Aug. 6, 2013, 1:16 AM), http://www.huffingtonpost.com/2013/08/05/dea-surveillance-cover-up_n_3706207.html (reporting data sharing between NSA and DEA).

208. Charlie Savage & Edward Wyatt, *U.S. Is Secretly Collecting Records of Verizon Calls*, N.Y. TIMES, June 5, 2013, http://www.nytimes.com/2013/06/06/us/us-secretly-collecting-logs-of-business-calls.html.

209. *Id.*

210. *Id.*

211. Claire Cain Miller, *Secret Court Ruling Put Tech Companies in Data Bind*, N.Y. TIMES, June 13, 2013, http://www.nytimes.com/2013/06/14/technology/secret-court-ruling-put-tech-companies-in-data-bind.html (reporting on Yahoo's objection to surveillance order).

212. *Id.*

213. *See id.* Reports regarding the FISC's deference to surveillance applications were also surfacing around this same time. It was reported that between 2008 and 2012, only two FISA warrant applications were rejected out of a staggering total of 8591. *See id.*

214. *See* 133 S. Ct. 1138, 1145-46 (2013).

215. *See id.* at 1146. In particular, the plaintiffs feared:

> (1) the Government will decide to target the communications of non-U.S. persons with whom they communicate; (2) in doing so, the Government will choose to invoke its authority under § 1881a

concluding the plaintiffs' claims "relie[d] on a highly attenuated chain of possibilities, [and did] not satisfy the requirement that threatened injury must be certainly impending."[216]

In *Clapper*, the Court relied on *United States v. United States District Court*, in which the defendants were charged with bombing a CIA office in Michigan.[217] The defendants moved to compel the United States to disclose certain surveillance information; however, the Government argued that the wiretaps in question were necessary to protect the nation from domestic attacks and therefore should not be disclosed.[218] The Court rejected the Government's argument, stating that there was "no reason to believe that federal judges will be insensitive to or uncomprehending of the issues involved in domestic security cases."[219] The Court also rejected the idea that "prior judicial approval will fracture the secrecy essential to official intelligence gathering."[220] In short, the Court held that prior judicial approval of the surveillance was required under the Fourth Amendment for the particular surveillance involved in this case, and although it may create an extra burden, "this inconvenience is justified in a free society to protect constitutional values. . . . [and] the Government's domestic surveillance powers will [not] be impaired to any significant degree."[221]

> rather than utilizing another method of surveillance; (3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures satisfy § 1881a's many safeguards and are consistent with the Fourth Amendment; (4) the Government will succeed in intercepting the communications of respondents' contacts; and (5) respondents will be parties to the particular communications that the Government intercepts.

Id. at 1148.

216. *Id.*; *see* Laird v. Tatum, 408 U.S. 1, 12-13 (1972) (holding constitutional claim necessitates showing of specific future harm for standing purposes).

> Stripped to its essentials, what respondents appear to be seeking is a broad-scale investigation, conducted by themselves as private parties armed with the subpoena power of a federal district court and the power of cross-examination, to probe into the Army's intelligence-gathering activities, with the district court determining at the conclusion of that investigation the extent to which those activities may or may not be appropriate to the Army's mission.

Laird, 408 U.S. at 14.

217. *See Clapper*, 133 S. Ct. at 1143 (citing United States v. U.S. Dist. Court, 407 U.S. 297 (1972)); United States v. U.S. Dist. Court, 407 U.S. 297, 299 (1972).

218. *See U.S. Dist. Court*, 407 U.S. at 299-301.

219. *Id.* at 320. The Court stated, "courts can recognize that domestic security surveillance involves different considerations from the surveillance of 'ordinary crime.' If the threat is too subtle or complex for our senior law enforcement officers to convey its significance to a court, one may question whether there is probable cause for surveillance." *Id.*

220. *Id.*

221. *Id.* at 321.

D. Privacy Statutes

Congress and state legislatures have been active in efforts to protect individual privacy. FOIA exempts personal, medical, and other files where disclosure would constitute an unwarranted invasion of privacy.[222]

In *United States Department of Justice v. Reporters Committee for Freedom of the Press*, the plaintiffs sought access to criminal records maintained by the FBI, and presented the question of whether the disclosure of such files to a third party constituted an unwarranted invasion of personal privacy within the meaning of FOIA.[223] The Court held, "as a categorical matter that a third party's requests for law enforcement records or information about a private citizen can reasonably be expected to invade that citizen's privacy, and that when the request seeks no 'official information' about a Government agency . . . the invasion of privacy is 'unwarranted.'"[224]

Other important federal statutes concerning privacy include the Privacy Act of 1974 (Privacy Act), which protects individuals from an intrusive federal government.[225] The Privacy Act establishes a regulated mechanism for requesting access to personally-identifiable information maintained by federal agencies. Individuals are permitted certain access to the records pertaining to them and request amendments to such information as applicable, and any disclosures of this information to third parties requires individual consent unless one of the statutory exemptions applies.[226] In addition, the agencies creating, maintaining, using, or disseminating identifiable personal data must assure the reliability of the data for its intended purpose and must take precautions to prevent misuse.[227] The Electronic Communications Privacy Act of 1986 amended the Privacy Act and expanded the scope of existing federal wiretap laws to include protection for all electronic communications.[228] It also eliminated the requirement that communications be transmitted via common carrier in order to receive protection.[229]

The FCRA protects consumers from the disclosure of inaccurate and arbitrary personal information held by consumer reporting agencies.[230] The information covered by this statute may only be released to a third party with the written consent of the individual or when there is reason to believe the requesting party intends to use the information for purposes of credit,

222. *See* 5 U.S.C. § 552(b)(6) (2012).
223. *See* 489 U.S. 749, 751 (1989).
224. *Id.* at 780.
225. *See generally* Privacy Act of 1974, 5 U.S.C. § 552a (2012).
226. *See id.*. § 552a(b)-(d) (stating conditions on disclosure of personally-identifiable information).
227. *See id.* § 552a(e) (stating agency obligations with respect to personally-identifiable information).
228. *See generally* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 110 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).
229. *See* 18 U.S.C. § 2510(1) (2012).
230. *See generally* Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x (2012).

employment, or insurance evaluation; in connection with the grant of a license or other government benefit; or for another "legitimate business need" involving the consumer.[231]

In 2003, the FCRA was modified by FACTA to help address problems of identity theft, and to make it easier for consumers to correct their credit information.[232] Pursuant to these changes, consumers are able to request that credit reporting agencies place "fraud alerts" in their files if they have been or are about to become victims of fraud or a related crime, such as identity theft.[233] Other notable federal statutory protections concern the privacy of census data,[234] driver's license information,[235] taxpayer information,[236] and much other information.[237]

E. Recent Developments

Following the NSA surveillance program leaks attributable to Edward Snowden, the American Civil Liberties Union (ACLU) filed a lawsuit challenging the agency's vast phone surveillance practices—the so-called "dragnet" network.[238] The agency program affected the ACLU because it was a customer of Verizon. The ACLU alleged the NSA's surveillance program undermined its ability to "engage in legitimate communications with clients, journalists, advocacy partners, and others."[239] Moreover, the ACLU claimed that such an expansive metadata collection was "likely to have a chilling effect on whistleblowers and others who would otherwise contact" its organization.[240] On December 27, 2013, Judge William H. Pauley III, granted the NSA's motion to dismiss the ACLU's complaint finding the NSA's bulk telephone metadata program lawful.[241] The ACLU has appealed this decision to the

231. *See id.* § 1681b (setting forth permissible uses of consumer-credit information).

232. *See generally* Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (codified as amended in scattered sections of 15 and 20 U.S.C.).

233. *See* 15 U.S.C. § 1681c-1 (2012) (describing process for requesting fraud alerts).

234. *See* 13 U.S.C. § 9 (2012) (proscribing certain uses of census data).

235. *See* 18 U.S.C. § 2721 (2012) (privatizing motor vehicle and license registration records).

236. *See* 26 U.S.C. § 7213 (2012) (penalizing unauthorized inspections of tax returns or other related information).

237. *See generally Privacy*, ELECTRONIC PRIVACY INFO. CENTER, http://epic.org/privacy (last visited Mar. 12, 2014) (listing various privacy regulatory topics in United States).

238. *See* Complaint at 10, Am. Civil Liberties Union v. Nat'l Sec. Agency, No. 13 Civ. 3994 (S.D.N.Y. June 11, 2013), *available at* https://www.aclu.org/national-security/aclu-v-clapper-legal-documents; *see also* Jacob Chamberlain, *ACLU Sues Obama Administration Over NSA 'Dragnet' Surveillance Revealed in Historic Leaks*, COMMON DREAMS (June 11, 2013), https://www.commondreams.org/headline/2013/06/11-8 (summarizing allegations in ACLU complaint).

239. Chamberlain, *supra* note 238.

240. *Id.*

241. *See* Memorandum and Order at 53, Am. Civil Liberties Union v. Nat'l Sec. Agency, No. 13 Civ. 3994 (S.D.N.Y. Dec. 27, 2013), *available at* https://www.aclu.org/national-security/aclu-v-clapper-legal-documents.

Court of Appeals for the Second Circuit.[242]

F. Summary

Concerns about governmental intrusion into homes fueled our separation from England. Early Fourth Amendment cases linked the inviolability of person, home, papers, and affects to the prohibitions against forced incriminations. *Boyd* and the dissent in *Olmstead* warned about a future where new means of invading the privacy of home and person would be developed.[243] Vesting power in the state would inevitably lead to overreaching and abuse.

In *Katz*, the fact that the caller was in a glass telephone booth for the entire world to see did not diminish the expectation that his conversation would be private.[244] The same reasoning applied to the heat monitors in *Kyllo*—the fact that one takes a hot bath, cooks hot food, or makes hot love should not be publicly available.[245] More recently, drug-sniffing dogs were held to be appropriate tools for surveillance in certain circumstances, and seizures of blood followed by laboratory analysis can provide extensive health data.[246] The Court limited the use of DNA collection without a warrant for identification purposes only by equating it to the collection of fingerprints. However, DNA collection arguably discloses much more information about an individual than fingerprints do. Finally, the pen-register seizure intrudes into one's call list, but leaves the content of the conversation inviolate, and therefore, does not constitute a Fourth Amendment search.[247]

Similar to the Court's First Amendment jurisprudence, national security exceptions are also found within the context of the Fourth Amendment. The combination of the USA PATRIOT Act and FISA and its subsequent amendments have granted our federal security agencies the extraordinary power to seize the electronic communications of the whole country.[248] The pretext for much of this broad authority has been the threat of additional terrorist attacks following those that brought down the World Trade Center towers.[249] In *Clapper*, the Court refused the opportunity to examine the merits of the Fourth Amendment claim, which suggests FISA warrants will continue

242. *See* Notice of Appeal at 1, Am. Civil Liberties Union v. Nat'l Sec. Agency, No. 13 Civ. 3994 (S.D.N.Y. Jan. 2, 2014), *available at* https://www.aclu.org/national-security/aclu-v-clapper-legal-documents.

243. *See generally* Olmstead v. United States, 277 U.S. 438 (1928), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967); Boyd v. United States, 116 U.S. 616 (1886).

244. *See* Katz v. United States, 389 U.S. 347, 353 (1967).

245. *See* Kyllo v. United States, 533 U.S. 27, 38 (2007).

246. *See generally* Missouri v. McNeely, 133 S. Ct. 1552 (2013); Florida v. Jardines, 133 S. Ct. 1409 (2013).

247. *See* Smith v. Maryland, 442 U.S. 735, 742-46 (1979).

248. *See supra* notes 194-205 and accompanying text (discussing authority granted under FISA and USA PATRIOT Act).

249. *See supra* Part III.C (explaining how national security issues influence Court's Fourth Amendment analysis).

to go unchecked.[250] As a consequence, the government's expansion of surveillance and construction of institutions of a surveillance state will make judicial review more difficult when questions similar to those put forth in *Clapper* are presented to the Court in the future. The Court would be well-advised to recall the following bold words from *United States v. United States District Court*:

> History abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.' Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent. . . . The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation.[251]

IV. CONCLUSION

The Court's First Amendment jurisprudence has expanded to cover speech in the form of information. The sources of information have an almost infinite variety, including maps, almanacs, dictionaries, shop manuals, instructional videos on YouTube, astronomy charts, baseball league standings in the sports pages, and so on.[252] The Internet places the history of knowledge and experience of the human race at the fingertips of anyone with access to a computer, and it has also caused an explosion in human interaction and communication. Laws and regulations concerning the access to and privacy of

250. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1140-1142 (2013) (bypassing NSA program scrutiny because plaintiffs' lacked standing).

251. United States v. U.S. Dist. Court., 407 U.S. 297, 314 (1972).

252. *See* Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 66-70 (2014) (describing nearly infinite varieties of data constituting speech). Bambauer uses the following illustration to show how seemingly innocuous items may become speech.

> There are many times that an event will leave a mark that has the potential to retell its story. A car may careen into a barrier and leave a streak of paint. Long after the car is towed, the streak states, in a way, when and where a crash occurred, how fast the car was traveling during impact, and what color the car was. The streak of paint can be received and interpreted by a human to create knowledge. But if a city repainted the barrier, we would not interpret this as a decision related to speech.

Id. at 58-59.

this information have grown as well. The First Amendment generally encourages openness, disclosure and the movement of information, while the Fourth Amendment protects the individual against the unwarranted and unwelcome seizures of information that may cause harm.

One of the central metaphors for the First Amendment is the marketplace of ideas.[253] In a commercial market, the buyer has an opportunity to compare available goods in terms of price and quality—quality products thrive and shabby ones are driven from the marketplace. "The marketplace [of ideas] is expected to include 'the widest possible dissemination of information from diverse and antagonistic sources.'"[254] Information flows into the marketplace of ideas and gets used in support of ideology or for commercial advantage. Accurate information increases the cost of maintaining a false belief. In *New York Times v. Sullivan*, Justice Brennan declared, "erroneous statement is inevitable in free debate, and . . . it must be protected if the freedoms of expression are to have 'breathing space' that they 'need . . . to survive . . . .'"[255] The hopeful result is the instruction of the listeners who have the good sense to pursue the good and true. Commercial marketplaces require the rule of law. Theft and sharp business practices must be punished. Safe passage must be guaranteed. Credit transactions must be enforced. Speakers need protection against violence. Hate speech and threats must be eliminated. Hackers, defrauders, and producers of viruses need to be thwarted. Personal information must be protected.

A second justification for free speech is that it facilitates democracy in two ways. First, organization, association, speech, and debate are critical to informing the electorate about the issues and the candidates so its members can cast a well-informed ballot.[256] Second, a well-functioning democracy requires that the public be informed about the conduct of public affairs in the hands of public officials.[257] Jeremy Bentham suggested that government secrecy is the instrument of conspiracy and often signals corruption or a desire to avoid accountability.[258]

253. *See* Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting) (referring to "free trade in ideas"); Bambauer, *supra* note 252, at 91-93.

254. Bambauer, *supra* note 252, at 92 (quoting Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 791 (1985)).

255. 376 U.S. 254, 271-72 (1964) (second alteration in original) (quoting NAACP v. Button, 371 U.S. 415, 433 (1963)).

256. *See* ALEXANDER MEIKLEJOHN, FREE SPEECH AND ITS RELATION TO SELF-GOVERNMENT 15-16 (1948) (illustrating town meeting analogy).

257. *See generally* JEREMY BENTHAM, *An Essay on Political Tactics*, *in* 2 THE WORKS OF JEREMY BENTHAM 299 (John Bowring ed., Edinburgh, William Tait 1843).

258. *See id.* at 310.

> Suspicion always attaches to mystery. It thinks it sees a crime where it beholds an affectation of secresy; and it is rarely deceived. For why should we hide ourselves if we do not dread being seen? In proportion as it is desirable for improbity to shroud itself in darkness, in the same proportion is it

A third justification arises from natural law. The individual presents herself to the world through a wide variety of expression. Knowledge and intelligence aid choice, morals, and the exercise of freedom and free will. Communication among members of a community leads to progress, cooperation, and peace.[259] A pluralistic society draws benefit from diversity of opinion and multiculturalism.[260]

A surveillance state engages in the systematic and routine collection of personal data.[261] As such, its presence will intimidate speakers and interfere with the marketplace of ideas. It changes the power relationships between people: surveillance provides the surveillor with information about the surveillee thereby empowering the former to use the new information to influence, manage, or control the surveillee.[262] In turn, putting the surveillor in a superior position alters the normal reciprocal relationship between strangers meeting as equals on their own terms.[263] Thus, the surveillor is in a position to manipulate the surveillee in multiple ways.[264] The most blatant example is blackmail, which can of course be practiced both subtly and viciously.[265] When surveillance uncovers some kind of wrongdoing on the part of the surveillee, the surveillor holds a position of power.[266] The surveillor comes to understand the psychology and the preferences of the surveillee.[267] We have seen this come to fruition through modern marketing practices, which track the preferences of targeted demographics to maximize sales.[268] Finally, big data miners can constantly comb through data for the purpose of discovering patterns in group behavior. [269]

Surveillance chills speech and with it the marketplace of ideas; it will disable the checks on government; self-expression will become self-conscious; the egalitarianism of technology will be undermined. Its purpose of influence, management, protection, or direction will generate the recognition and

> desirable for innocence to walk in open day, for fear of being mistaken for her adversary. So clear a truth presents itself at once to the minds of the people, and if good sense had not suggested it, malignity would have sufficed to promulgate it. The best project prepared in darkness, would excite more alarm than the worst, undertaken under the auspices of publicity.

Id.

259. *See* David A. J. Richards, *Free Speech and Obscenity Law: Toward a Moral Theory of the First Amendment*, 123 U. PA. L. REV. 45, 62 (1974) (explaining contractarian theory of First Amendment).

260. *See* LEE BOLLINGER, THE TOLERANT SOCIETY 9-10, 120 (1986).

261. *See* Richards, *supra* note 3, at 1937.

262. *See id*. at 1952-53.

263. *See id.* at 1953.

264. *See id.*

265. *See* Richards, *supra* note 3, at 1953-54.

266. *See id.* at 1954-55.

267. *See id.* at 1955-56.

268. *See id.* at 1955.

269. *See* Richards, *supra* note 3, at 1956-57.

resistance of speakers.[270] Recall Orwell's thought crime, which was deterred by constant state surveillance personified by Big Brother.[271] Of course the proponents of the surveillance state claim that it is an effective means for keeping us all safe. Just how dangerous is the threat of foreign and domestic terrorism? Is it more dangerous than the earlier threats of worldwide communism, or fascism, or syndicalism, or other enemies real or imagined? Is it more dangerous than our own paranoia? Is it more dangerous than having to face the American national security establishment composed of the NSA, FBI, CIA and the national defense establishment without the protections of the First and Fourth Amendments?

270. *See* DAVID LYONS, SURVEILLANCE STUDIES: AN OVERVIEW 23 (2007); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 816 (2004).

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