Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground

Avner Levin* and Mary Jo Nicholson†

PRIVACY AND PERSONAL INFORMATION are regulated differently in the European Union (EU), the United Sates (US) and Canada. The EU and Canada centrally supervise the private sector's use of personal data, whereas the US regulation of the private sector is minimal. These differences emanate from distinct conceptual bases for privacy in each jurisdiction. In the US, privacy protection is essentially liberty protection, *i.e.* protection from government. For Europeans, privacy protects dignity or their public image. In Canada, privacy protection is focused on individual autonomy through personal control of information. We propose the Canadian model as a conceptual middle ground between the EU and the US, as a basis for future American privacy protection.

LA VIE PRIVÉE ET LES RENSEIGNEMENTS personnels sont régis différemment dans l'Union européenne, aux États-Unis et au Canada. L'Union européenne et le Canada exercent une supervision centrale sur l'utilisation des données personnelles par le secteur privé, alors que la réglementation du secteur privé aux États-Unis est minimale. Ces différences découlent d'une vision conceptuelle distincte de la vie privée dans chacun de ces ressorts. Aux États-Unis, la protection de la vie privée est liée essentiellement à la protection de la liberté, c'est-à-dire la protection contre le gouvernement. En contexte européen, la protection de la vie privée est centrée sur la protection de la dignité et de l'image publique. Au Canada, la protection de la vie privée est axée sur l'autonomie individuelle par le contrôle personnel des renseignements. Nous proposons le modèle canadien, qui se situe à mi-chemin entre les conceptions européenne et américaine, en tant que fondement de la protection de la vie privée en Amérique dans l'avenir.

* BSc, LLB, LLM, SJD. Assistant Professor, Law Area, Faculty of Business, Ryerson University.

† BA, LLB, LLM. Professor, Law Area, Faculty of Business, Ryerson University.

Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground

Avner Levin and Mary Jo Nicholson

1. INTRODUCTION

TRADITIONALLY, AMERICANS HAVE PREFERRED that their government leave them alone. They value "life, liberty and the pursuit of happiness,"[1] and do not admire nations such as Canada with its belief in "peace, order and good government."[2] Americans do not understand why the EU and Canada have created a government watchdog to ensure the privacy of their citizens, for surely privacy is ensured only when government leaves one alone.[3] Recent global events, the spectre of terrorism since 9/11, and the consequent passage in the US of the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* (USA PATRIOT Act),[4] have combined to strengthen American concerns that privacy must be protected, first and foremost, from "Big Brother" government.[5] We shall argue below that focusing solely on protecting one's privacy from government, based as it is on an American understanding of privacy as liberty, does the American public a disservice. Americans need now, more than ever, to protect their privacy not only from government, but from private sector abuse as well. Nowhere is this more evident than in the emerging field of personal data protection where American

---

1. United States, *Declaration of Independence* (1776), <http://www.archives.gov/national_archives_experience/charters/print_friendly.html?page=declaration_transcript_content.html&title=NARA%20%7C%20The%20Declaration%20of%20Independence%3A%20A%20Transcription>.
2. *Constitution Act, 1867* (U.K.) 30 & 31 Vict. C.3, s. 91, reprinted in R.S.C. 1985, App. II, No. 5, <http://laws.justice.gc.ca/en/const/c1867_e.html#executive>.
3. Canada has created the office of Federal Privacy Commissioner, and there are also provincial Privacy Commissioners. In Europe, there is a European Data Protection Supervisor as well as privacy regulators in every European Union member, and, where those members are federations themselves (*e.g.* Germany), at the federal and state levels.
4. Pub. L. No. 107-56, 115 Stat. 272 (2001), <http://www.usdoj.gov/eoir/vll/legislation/hr3162.pdf> [PATRIOT Act].
5. There are voices in the US that continue to question the absence of omnibus private sector regulation, and we shall discuss them in greater detail below. See *e.g.* Marsha Cope Huie, Stephen F. Laribee & Stephen D. Hogan, "The Right to Privacy in Personal Data: The EU Prods the US and Controversy Continues" (2002) 9 Tulsa Journal of Comparative & International Law 391, <http://www.utulsa.edu/law/ilj/vol9no2.htm>; Joel Reidenberg, "E-Commerce and Trans-Atlantic Privacy" (2001) 38 Houston Law Review 717, <http://www.houstonlawreview.org/archive/downloads/38-3%20pdf%20files/HLR38P717.pdf>.

privacy is increasingly threatened by the collaboration of government with private sector data brokers. We shall argue that Americans need to take their lead from the EU and from their *North American Free Trade Agreement* (NAFTA) partner, Canada, and such change is conceivable if Americans could envision their privacy not only in terms of their liberty and freedom, but in terms of their control over their public persona and their dignity. It is exactly this form of control that was advocated by Warren and Brandeis in their seminal article "The Right to Privacy"[6] and the time has finally come for the US to heed their call.

Privacy is protected in the US by means of a patchwork quilt made up of common law, federal legislation, the US Constitution, state law, and certain state constitutions. In the first section of this paper we review this quilt and contrast it with the more uniform, although not perfect, approaches of the EU and Canada. There are many reasons for the differences in the three jurisdictions' approaches to privacy protection, ranging from global economic forces to local politics. Indeed, it would be simplistic to argue that analyzing privacy protection from a single perspective would necessarily bring greater clarity to these differences. The scope of this paper necessitates such limits, however, and in its second section we focus on the conceptual underpinnings of privacy in the US, the EU, and Canada. We find, unsurprisingly perhaps, that the concepts on which privacy is based in each of these jurisdictions play a significant role in their legal protection of privacy. In the US, we find privacy protection to be primarily motivated by the protection of liberty. In the EU, we find that the protection of privacy is mainly the protection of one's dignity. In Canada, we find that Canadians occupy the middle ground between the EU and the US, sharing American concerns about "Big Brother" government, while also having deep concerns about private sector abuse of their personal information. As a result, we find Canadians identify privacy with a sense of control that enables them as individuals to set limits upon both the public and the private sector. This analysis of privacy provides us with a better understanding of the regulatory differences between the US and the EU, and offers Americans the possibility of a middle ground, modelled on the Canadian approach to privacy. The Canadian conceptual middle ground that we will attempt to demonstrate is particularly well suited, we believe, for Americans concerned with the erosion of their privacy by their private sector, whether in collaboration with their government or not. In such a case, some American trust in "good government," one that will provide them not only liberties but also personal control, might go a long way to ensure their privacy not only from government, but from their fellow Americans as well.

---

6. Samuel D. Warren & Louis Brandeis, "The Right to Privacy" (1890) 4 Harvard Law Review 193, <http://www.louisville.edu/library/law/brandeis/privacy.html> [Warren & Brandeis].

*

2. DIFFERENT APPROACHES TO PROTECTION OF PRIVACY IN THE THREE JURISDICTIONS EXAMINED

2.1 The United States and its Respect for the Discipline of the "Marketplace"

THE LEGAL FRAMEWORK FOR PRIVACY in the United States is somewhat disjointed and piecemeal. Privacy provisions exist in common law, in the federal and state constitutions, and in a variety of statutes addressing specific issues that have arisen in different sectors and jurisdictions. Compared to the example set by the EU, common law and constitutional protection for informational privacy is somewhat unpredictable.[7] As a consequence, it is difficult to articulate any overall legal theory with respect to privacy.[8]

Generally, the privacy of physical space or things, receives strong protection through privacy tort claims.[9] The privacy torts are not, however, readily applicable to misuse of personal information unless the information was taken from the victim directly or from some other private source, such as the victim's bank account.[10] While the Constitution protects personal information against government intrusion, the interest in avoiding disclosure of personal matters does not seem very broad.[11] Statutes have filled in many of the holes left by the insufficiencies of common and constitutional law, but the disparate state and federal privacy statutes affecting informational privacy address narrow, specific issues rather than privacy as a concept.[12] In some respects, state legislatures have been the most promising venue for new informational privacy protections, but the effect of these is limited by jurisdictional limitations and the states' weak enforcement capabilities.[13]

This piecemeal approach is increasingly problematic in an environment in which information technology is expanding rapidly and affecting many areas of privacy law. The reactive, adaptive process adopted by the courts makes it

---

7. Will Thomas DeVries, "Protecting Privacy in the Digital Age" (2003) 18 Berkeley Technology Law Journal 283 at p. 285, believes that the legal theory connecting the various privacy protections is disjointed; and several branches of law have developed, all growing from the seed of privacy, but based on differing theories of what should be protected.

8. See Daniel J. Solove, "Conceptualizing Privacy" (2002) 90 California Law Review 1087, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=313103> at pp. 1088-1089.

9. Some authors believe that Warren and Brandeis's call for a right to privacy was merely to establish a privacy tort. See Jed Rubenfeld, "The Right of Privacy" (1989) 102 Harvard Law Review 737 at p. 752.

10. See DeVries, *supra* note 7 at p. 288, who states that courts are unlikely to find misuse of "non-private" personal information to be "highly offensive to a reasonable person" – the general standard for the privacy torts under the *Restatement (Second) of Torts* s. 652B (1977).

11. *Ibid.* DeVries discusses *Whalen v. Roe,* 429 U.S.589, <http://straylight.law.cornell.edu/supct/html/historics/USSC_CR_0429_0589_ZS.html>, 51 L. Ed. 2d 64 (1977) [*Whalen*] in which the Court refused to find that the government's recording of personal drug prescription information violated the constitutional right to privacy because the information was adequately protected.

12. See generally Marc Rotenberg, *The Privacy Law Sourcebook: United States Law, International Law, and Recent Developments* (Washington: EPIC Publications, 2003).

13. DeVries, *supra* note 7. See DeVries's discussion of California law providing residents with stronger protection of Social Security Numbers and credit fraud; *The Penal Code of California*, ss. 530.5-530.7 (2002), <http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=pen&codebody=&hits=20> and the *Criminal Code of Georgia* which prevents businesses from discarding records that may contain their customers' personal information (*Criminal Code of Georgia*, ss. 16-9-121, 127 (2002), <http://www.legis.state.ga.us/legis/GaCode/Title16.pdf>).

difficult to address digital privacy problems rationally or effectively. On the whole, the US legislation we discuss provides citizens with greater protection against the collection and use of personal information by government, as opposed to the private sector. It is significant, as we shall see, that the EU *Privacy Directive*[14] imposes limits on interactions in the market place. The US has been less willing to impose government restrictions on the private sector, and chooses to rely on market constraints, possibly reflecting Americans' traditional distrust of a centralized government.[15]

2.1.1. US Legislative Measures Affecting Privacy

It is impossible within the scope of this paper to discuss the many references to privacy found in state constitutions and legislation.[16] Accordingly, we limit our discussion to federal legislation, but the US piecemeal approach to privacy is readily demonstrated in our limited discussion. We have included legislation primarily protecting privacy from government, as well as legislation addressed primarily to the private sector.

2.1.1.1. Legislation protecting privacy from government

2.1.1.1.1. *The Privacy Act* of 1974[17]

This Act is the only federal omnibus Act that protects informational privacy. The *Privacy Act* applies only to data processing by the federal government and not to state governments or the private sector. The Act obliges federal agencies to collect information to the greatest extent possible directly from the concerned individual, to retain only relevant and necessary information, to maintain adequate and complete records, to provide individuals with rights of access to review and have their records corrected, and to establish safeguards to ensure the security of the information. The Act contains a significant exception in the

---

14. EC, *Council Directive 94/46EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data*, [1995] O.J.L. 28, <http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>.

15. Gregory Shaffer, "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards" (2000) 25 Yale Journal of International Law 1, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=531682> at p. 6, and Peter Swire & Robert Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (Washington: Brookings Institution Press, 1998), <http://brookings.nap.edu/books/081578239X/html/> at p. 153, who observe that Americans historically have a strong suspicion of government and a relatively strong esteem for markets and technology, while Europeans have given government a more prominent role in fostering social welfare but have placed more limits on unfettered development of markets and technology. European governments regulate themselves less strictly with respect to open meetings and freedom of information laws, whereas they are stricter with respect to regulating the press and other private sector users of information.

16. For example, the constitutions of California, C.A. Const. art. 1, s. 1, <http://www.leginfo.ca.gov/.const/.article_1>; Alaska, Alaska Const. art. 1, s. 22, <http://ltgov.state.ak.us/constitution.php?section=1>; Florida, Fla. Const. art. 1, s. 23, <http://www.leg.state.fl.us/Statutes/index.cfm?Mode=Constitution&Submenu=3&Tab=statutes#A01S23>; and Illinois, Ill. Const. art. 1, s. 6, <http://www.ilga.gov/commission/lrb/con1.htm> proclaim a right to privacy.

17. 5 U.S.C. s. 552a, <http://assembler.law.cornell.edu/uscode/html/uscode05/usc_sec_05_00000552---a000-.html>.

form of the "routine use exception" that permits federal agencies to transfer information between themselves for what they justify as a "routine use." Since the Act does not apply to private sector databases, federal agencies have increasingly relied on them.[18]

2.1.1.1.2. *The Electronic Communications Privacy Act* of 1986 (ECPA)[19]

The ECPA requires government officials who wish to intercept or obtain electronic communications—such as email or other information available electronically, such as Internet Service Providers (ISP) logs and public library patron records—to seek and receive permission, known as a "Title III" order, from a federal judge. The ECPA has been amended by the USA PATRIOT Act, which we discuss separately below.

2.1.1.1.3. *The Privacy Protection Act* of 1980[20]

Despite its title, this Act serves to protect free speech and First Amendment rights, not privacy in general. The Act prohibits government from searching or seizing any work or materials held by a person intending to disseminate it to the public in some form of public communication (*e.g.* newspapers, books, broadcasts) without court authorization (*e.g.* a subpoena). There has not been any ruling yet as to whether the Act applies to forms of electronic communication such as message boards.

2.1.1.1.4. *The Family Educational Rights and Privacy Act* (FERPA)[21]

This Act, passed in 1974, protects the privacy of student records at all educational institutions receiving federal funding (*e.g.* universities and colleges.) Educational institutions cannot disclose student records or personal information to third parties without consent, and must grant the students access to such information held by the institution. Students have the right to challenge and amend inaccurate records. FERPA was amended by the PATRIOT Act, as we discuss below.

---

18. Although the Act applies to private sector databases which are created at the request of government *(e.g.* by outsourcing), it does not apply to private sector databases that already exist and which government merely requests to access. Privacy advocates argue that this constitutes a convenient loophole in the Privacy Act which both federal agencies and database companies (known as Commercial Data Brokers) exploit. See Chris Hoofnagle, "Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement" (2004) 29 North Carolina Journal of International Law & Commercial Regulation 595; Jim Dempsey, "Privacy's Gap: The Largely Non-Existent Legal Framework for Government Mining of Commercial Data," The Center for Democracy and Technology (28 May 2003), <http://www.cdt.org/security/usapatriot/030528cdt.pdf>.

19. Pub. L. No. 99-508 100 Stat. 1848 at p. 1868, <http://www4.law.cornell.edu/uscode/html/uscode18/usc_sup_01_18_10_I_20_119.html>.

20. 42 U.S.C. s. 2000aa (1980), <http://assembler.law.cornell.edu/uscode/html/uscode42/usc_sec_42_00002000--aa000-.html>.

21. 20 U.S.C. s. 1232g (1974), <http://assembler.law.cornell.edu/uscode/html/uscode20/usc_sec_20_00001232---g000-.html>.

2.1.1.1.5. *The Driver's Privacy Protection Act*[22]

This Act of 1994 prohibits the public disclosure of personal information contained in state department of motor vehicle records for marketing purposes, unless drivers expressly consent. The Act was challenged as unconstitutional (Congress interfering in state-jurisdiction), but was upheld by the Supreme Court. Personal information can still be disclosed for many other purposes (*e.g.* private investigations, toll payment, identity confirmation) without consent, so the Act, despite its title, only offers limited protection to drivers.

2.1.1.1.6. *The Right to Financial Privacy Act*[23]

The *Right to Financial Privacy Act* was designed to protect the confidentiality of personal financial records, but only from government. The Act essentially provides statutory Fourth Amendment protection to bank records (*i.e.* law enforcement agencies cannot access or seize records without some form of authorization such as a warrant). Furthermore, financial institutions cannot obtain "blanket" consent from customers to release records as a condition of doing business. Customers also have a right to access a record of all disclosures made of their personal information.

2.1.1.2. Legislation protecting privacy in the private sector

2.1.1.2.1. *The Fair Credit Reporting Act* (FCRA)[24]

Another Act addressing the realm of personal finances is the FCRA. The FCRA was originally passed in 1970, amended in 1996, and most recently amended in 2003.[25] It authorizes the Federal Trade Commission (FTC) to regulate the private sector in the area of credit reporting. Businesses reporting credit (known as Consumer Reporting Agencies) are obligated to report credit information accurately and fairly, to correct any errors in their reports, and to include a consumer's dispute of their credit record as part of the report. Although the FCRA recognizes the consumer's right to privacy, and some measures in the FCRA do address privacy (*e.g.* the consumers have a right to access their records, albeit for a fee), the FCRA is primarily concerned with ensuring credit accuracy.[26] This purpose of the FCRA is compatible, of course, with the overall goal of increasing marketplace efficiency—and consumers, at the end of the day,

---

22. 18 U.S.C. s. 2721 (1994),<http://assembler.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002721----000-.html>.
23. 12 U.S.C. s. 35 (1978), <http://assembler.law.cornell.edu/uscode/html/uscode12/usc_sec_12_00003401----000-.html>. The Act was passed in response to *United States v. Miller,* 425 U.S. 435, <http://www.justia.us/us/425/435/index.html>, where the Supreme Court decided that an individual has no reasonable expectation of privacy in information provided to others. *Miller* is still applicable to personal information not governed by the Act.
24. 15 U.S.C. s. 1681 (1970), <http://assembler.law.cornell.edu/uscode/html/uscode15/usc_sec_15_00001681----000-.html>.
25. This latest amendment is also known as the *Fair and Accurate Credit Transactions Act* (FACT Act).
26. The measures in the Act do not apply to information contained in credit reports that is available elsewhere, such as names and addresses.

cannot prevent Consumer Reporting Agencies from forwarding their credit reports to any person with a "legitimate" interest, such as potential employers or insurance companies.

2.1.1.2.2. *The Financial Modernization Act*[27]

This recent Act (1999), more commonly known as the *Gramm-Leach-Bliley Act* (GLBA), is the first to attempt some form of privacy regulation in the financial sector, rather than simply restrict government access to financial information or ensure market efficiency, as the Acts above. The Act requires that financial institutions have a privacy policy and that they bring it to their customers' attention. Although financial institutions are broadly defined (*e.g.* car dealerships offering leases are included), the legislation fails to set any principles for those policies. Customers are able to opt-out—that is, stipulate to their financial institutions that they do not want their personal information to be shared with other businesses in certain circumstances. Nonetheless, affiliated businesses may share information freely. The Act is administered by the Federal Trade Commission (FTC).

2.1.1.2.3. *The Identity Theft and Assumption Deterrence Act*[28]

This Act, enacted in 1998, criminalizes the unauthorized use for a felonious purpose of another person's identity, and provides for penalties of up to fifteen year imprisonment and a maximum fine of US$250,000. It establishes that the person whose identity was stolen is a victim and allows this victim to seek restitution (previously, only businesses [*e.g.* financial institutions], which suffered monetary losses, were considered victims). The Act is administered by the FTC. Note that the Act does not provide protective measures for privacy. Rather, it creates criminal sanctions for invasion of privacy in order to deter identity theft.

2.1.1.2.4. *The Cable Communications Policy Act*[29]

This Act regulates the cable industry in the US generally, and incorporates several specific privacy measures. Cable companies are not allowed to collect personal information without consent, or to disclose it to third parties, unless the information is necessary for service purposes. Together with the following Act, it is an example of the American piecemeal approach to privacy of personal information.

---

27. 15 U.S.C. s. 6801-6809 (1999), <http://www.law.cornell.edu/uscode/html/uscode15/usc_sup_01_15_10_94_20_I.html>.
28. 18 U.S.C. s. 1028 (1998), <http://assembler.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001028----000-.html>.
29. 47 U.S.C. s. 551 (1984), <http://assembler.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000551----000-.html>.

2.1.1.2.5. *The Videotape Privacy Protection Act*[30]

This Act was passed due to the controversy surrounding the release of Judge Bork's video rental records during his failed Supreme Court nomination. The Act prohibits video stores from disclosing customer records without their consent. Furthermore, the Act requires video stores to destroy personal information within a year of the date that it is no longer necessary for the purpose for which it was collected. The Act is under review by the US Supreme Court.

2.1.1.2.6. *The Telephone Consumer Protection Act*[31]

This Act, enacted originally in 1991 and amended since, sets the legislative basis for the Federal Communications Commission (FCC) to establish a "do-not-call" list for telemarketers. Telemarketers are required under the Act to maintain such a list and abide by the wishes of listed consumers not to be called.

2.1.1.2.7. *The Telecommunications Act of 1996*[32]

Within the *Telecommunications Act* of 1996, which updated the *Communications Act of 1934*,[33] are specific privacy measures designed to limit marketing on behalf of telephone companies, based on their ability to access their customers' calling patterns. Telephone companies must obtain express consent from customers to use such data for marketing purposes, although the Act does not state how the consent is to be obtained. The Act is administered by the FCC.

2.1.1.2.8. *The Health Insurance Portability and Accountability Act* of 1996 (HIPAA)[34]

HIPAA sets out to eliminate "job-lock"—that is, the denial of employment based on medical information. In order to protect personal medical information traveling from healthcare providers and administrators to potential employers, *HIPAA* establishes privacy measures, which aim to be a minimal standard to which states can add. Personal health information in the hands of healthcare providers, health plans, and healthcare clearinghouses (*i.e.* data and billing processors, commonly referred to as "covered entities") cannot be disclosed without the patient's express consent.[35] Consent under HIPAA must be obtained

---

30. 18 U.S.C. s. 2710 (1988), <http://assembler.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002710----000-.html>.
31. 47 U.S.C. s. 227 (1991), <http://www.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000227----000-.html>.
32. 47 U.S.C. s. 609 (1996), <http://assembler.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000609----000-.html>.
33. 47 U.S.C. 151 (1934), <http://www.fcc.gov/Reports/1934new.pdf>.
34. Pub. L. No. 104-191, Stat. 1936 (1996), <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_bills&docid=f:h3103enr.txt.pdf>.
35. This method of consent is also known as an "opt-in" method, and is preferred by privacy advocates to the "opt-out" mechanism of the GLBA. See Bradley McMahon, "After Billions Spent to Comply with HIPAA and GLBA Provisions, Why is Identity Theft the Most Prevalent Crime in America?" (2004) 49 Villanova Law Review 625.

prior to treatment, yet it is not required for treatment, payment or other healthcare operations (*e.g.* delivery of medical equipment to a patient's home). Further, patients have a right to access and amend their information, and a right to know to whom the information has been provided. HIPAA is administered by the Office of Civil Rights in the Department of Health, which can impose both civil and criminal penalties of up to US$250,000 and 10 year imprisonment.

2.1.1.2.9. *The Children's On-line Privacy Protection Act* of 1998 (COPPA)[36]

COPPA was passed in 1998 to protect children's personal information from collection and misuse by commercial websites. COPPA requires commercial websites and other online services directed at children 12 and under, or websites which collect information regarding age, to provide parents with notice of their information practices and to obtain parental consent prior to the collection of personal information from the children. The Act further requires such sites to provide parents with the ability to review and correct the information about their children that was collected by such services. COPPA is administered by the FTC, and must be distinguished from several other acts passed in the US in recent years aimed at curbing child pornography, such as the *Communications Decency Act* of 1996 (CDA)[37]; the *Child Pornography Prevention Act* of 1996 (CPPA);[38] and the *Child Online Protection Act* of 1998 (COPA).[39] These Acts, as we discuss in the next section, have been attacked as unconstitutional by the private sector in the US since they infringe on First Amendment rights.

2.1.2. US Constitutional Concerns and Privacy

The absence of a constitutional right to privacy (particularly in light of its existence in several state constitutions) gives rise to two broad constitutional concerns regarding privacy. The first is that the US piecemeal approach will result in various privacy-protecting acts clashing with well-established constitutional rights. As a result, these Acts and their protection of privacy will be watered down if not stricken down outright. The second is that the US Constitution with its supporting body of jurisprudence does not provide adequate privacy protection, especially in light of continuing technological development. Privacy advocates fear that many such developments, such as public video surveillance, will, if they come before the courts, be simply ruled to be constitutional and the privacy right not "worthy" of the Constitution's protection in that context.[40]

---

36. Pub. L. No. 105-277, Div. C, Title XIII, 112 Stat. 2681-2728 (1998), <http://ftc.gov/ogc/coppa.htm>.
37. 47 U.S.C. s. 223(d) (1996), <http://www.cybercrime.gov/47usc223NEW.htm>, makes it a crime to display patently offensive messages or images to minors.
38. 18 U.S.C. s. 2256 (2000), <http://assembler.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002256----000-.html>.
39. 47 U.S.C. s. 231 (1998), <http://assembler.law.cornell.edu./uscode/html/uscode47/usc_sec_47_00000231----000-.html>, makes it illegal to use the World Wide Web to communicate material that is harmful to minors for commercial purposes.
40. See *e.g.* Marc Jonathan Blitz , "Video Surveillance and the Constitution of Public Space" (2004) 82 Texas Law Review 1329, <http://www.utexas.edu/law/journals/tlr/abstracts/82/82blitz.pdf>.

Discussions of privacy protection in light of the First Amendment exemplify the first broad concern we raise above. The constitutional right to free speech is very important to Americans, and any attempt to regulate the content of free speech is highly suspect under the First Amendment. The controversy in the US about freedom of the press and the more generalized freedom of speech is as old as the American colonies,[41] but until recently commercial interests in the main did not presume to invoke the First Amendment guaranty of freedom of speech as covering commercial speech. Over the last thirty years, however, there have been cases in which the private sector has successfully argued that legislation ostensibly protecting privacy imposes an unconstitutional restriction on free speech. Among the Acts attacked were the CDA, COPA and CPPA. All were declared unconstitutional by the courts.[42]

First Amendment rights are also relevant to privacy protection due to the well received view that the internet is the ultimate First-Amendment enabling technology because it allows anyone, regardless of wealth, status or political clout to share opinions with the world.[43] The idea that an Orwellian "Big Brother" would be authorized to monitor which websites an individual visits or what messages he or she sends through cyberspace is abhorrent to the American value of free speech, yet as we discuss below may not be so far-fetched in the context of the PATRIOT Act.[44]

As an example of the second broad constitutional concern, that the Constitution will ultimately prove to provide inadequate privacy protection, we consider the discourse of the privacy protection offered by the Fourth Amendment. The Fourth Amendment protects against "unreasonable searches and seizures" by government. Privacy advocates note, of course, that reasonable searches and seizures are permitted. That, in turn, has led the Supreme Court to consider what exactly reasonable expectations of privacy are.[45] For instance, consider video surveillance of public spaces.[46] Modern video cameras are not static devices with limited image storage on endlessly looping video tapes, but active devices that can be manipulated to trace an individual's movements within the camera zone, and that can communicate with each other to ensure continuous coverage as individuals move from one camera area to another. Furthermore, images can be digitally recorded for posterity. Currently, Americans' expectations are that they will not be monitored in public with such

---

41. See Huie *et al.*, *supra* note 5 at p. 12.
42. We discuss these decisions below and query whether they represent a weakening of the individual American's right to informational privacy, as some believe. See Huie *et al.*, *ibid.* at p. 13.
43. See Ric Simmons, "Technology Enhanced Surveillance by Law Enforcement Officials" (2004) Public Law & Legal Theory Working Paper Series, No. 10 (Moritz College of Law, Ohio State University), <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=539704>, quoting Senator Hatch, Committee Chairman of the Senate Judiciary Committee, speaking at hearings on "Carnivore" in September 2000. The Senator went on to advocate "properly calibrated laws" to protect privacy interests of all who use the internet, but at the same time ensure that the communications of criminals and terrorists by computers should not go undetected.
44. Of course, in the context of the PATRIOT Act, privacy advocates hope rather than fear that the Act will clash with the Constitution and be stricken or watered down.
45. *Katz v. United States*, 389 U.S. 347 <http://straylight.law.cornell.edu/supct/html/historics/USSC_CR_0389_0347_ZS.html> (1967) [*Katz*].
46. Discussed at length in Blitz, *supra* note 40.

cameras.[47] However, the very discussion of expectations in such a context is moot. The Supreme Court has ruled that there are no privacy expectations in public, which is the space covered by video cameras. Thus, the protection granted by the Fourth Amendment does not extend to such expectations of privacy.[48]

Consider other technological developments, known collectively as Location Awareness Technologies. Examples are Global Positioning Systems that can be worn on the person (known as Personal Locators), implanted under the skin, installed in vehicles and in cellular phones, in "black box" devices installed in vehicles, and in Inter-Vehicle Communication Devices.[49] Such technology raises privacy issues, not only with respect to government's use, but also with respect to the private sector and the extent to which employers, for instance, can monitor employees and their use of the "company car" and the "company phone,"[50] or to which marketing firms can "mine" data accumulated by Personal Locators.[51] None of these issues, however, currently falls under Fourth Amendment protection, mainly, again, because these technologies are primarily applied in public spaces.

Finally, there is of course the issue of searches and seizures conducted by new means, such as the development of DNA databases or the execution of "digital" searches.[52] The Fourth Amendment does not appear to offer effective privacy protection against these new forms of searches, and it appears, again, to have been closely circumscribed outside of the realm of physical privacy.[53] State entities have not been held to the same exacting standard with respect to digital searches as have been applied to physical searches and seizures. Thus, a number of privacy scholars have concluded that constitutional protection against government misuse of digital searching is minimal.[54] It is important to remember in this context, moreover, that while constitutional protection may be weak, protection has been, at least until now, provided to members of society primarily under the ECPA. We discuss below how this protection is affected by the

---

47. Christopher Slobogin, "Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity" (2002) 72 Mississippi Law Journal 213, <http://www.olemiss.edu/depts/law_school/ruleoflaw/pdf/LJournal02Slobog.pdf> at pp. 272-285.
48. Indeed, we shall discuss below whether it is the American conception of privacy, which is at stake in such circumstances or some other conceptually linked, yet distinct, notion of anonymity.
49. For a technology-oriented discussion see Jean-Pierre Hubaux, Srdjan âapkun & Jun Luo, "The Security and Privacy of Smart Vehicles" *IEEE Security and Privacy Magazine* 2:3 (2004) at p. 49.
50. See John Canoni, "Location Awareness Technology and Employee Privacy Rights" (2004) 30 Employee Relations Law Journal 26.
51. See Waseem Karim, "The Privacy Implications of Personal Locators: Why You Should Think Twice Before Voluntarily Availing Yourself to GPS Monitoring" (2004) 14 Washington University Journal of Law & Policy 485, <http://law.wustl.edu/Journal/14/p485Karimbookpages.pdf>.
52. For a summary of the constitutional issues regarding DNA databases see Bonnie L Taylor, "Storing DNA Samples of Non-Convicted Persons & The Debate Over DNA Database Expansion" (2003) 20 Thomas M. Cooley Law Review 509.
53. See *supra* note 7 at p. 308.
54. See *ibid.* at p. 307; Stephen A. Osher, "Privacy, Computers and the PATRIOT Act: The Fourth Amendment Isn't Dead, But No One Will Insure It" (2002) 54 Florida Law Review 521, <http://www.flr.law.ufl.edu/pdf/july2002/osher.pdf>; and Huie *et al.*, *supra* note 5 at p. 414.

amendments of the PATRIOT Act, since courts have had a tendency, particularly post 9/11, to dismiss privacy concerns when national security might be at stake.[55] For decades, in cases such as *Olmstead,*[56] *Katz,*[57] *Smith*[58] and *Kyllo,*[59] the US Supreme Court has struggled to balance law enforcement's legitimate need to capitalize on advances in electronic surveillance technology with an individual's constitutional right to be secure against unreasonable searches and seizures. How this balance will shift in light of present fears of terrorism remains to be seen.

2.1.3. The PATRIOT Act

The *Kyllo* case was decided in June 2001, just months before the attack on the World Trade Center and the Pentagon. Since 9/11 the protective and liberal attitude towards the importance of privacy rights has undergone a sea change in the United States. Within weeks of 9/11, Congress passed the USA PATRIOT Act. The PATRIOT Act amends several privacy-protecting Acts, as we have mentioned above, weakens their privacy protections and allows government greater invasions of privacy, ostensibly in order to intercept and obstruct terrorism.

The PATRIOT Act has effectively amended the ECPA to allow law enforcement officials to read the addresses of all the emails that are sent from a computer, and all websites visited.[60] Although the PATRIOT Act includes the proviso, "such information shall not include the contents of any communication," and therefore ostensibly precludes government access to the contents of specific electronic communications, the unique characteristics of internet addressing schemes make it possible for federal investigators to recreate an extraordinarily complete diary of a suspect's internet activities.[61] Under this legislation, it is possible to obtain information such as what websites a suspect has accessed and what topics he was searching for—all preserved in an evidentiary record that may

---

55. See DeVries, *supra* note 7 at p. 308.
56. In *Olmstead v. United States*, 277 U.S. 438, <http://straylight.law.cornell.edu/supct/html/historics/USSC_CR_0277_0438_ZS.html> (1928), the issue was whether government's use of technology to monitor telephone communications offended the Fourth Amendment's proscription against warrantless searches. The court decided by a 5-to-4 majority that the Fourth Amendment had not been violated because no physical intrusion of the home had occurred.
57. *Supra* note 45. *Katz* was decided thirty nine years after *Olmstead* and effectively changed the law as the Court held that electronic surveillance could violate the Fourth Amendment in the same way a physical search could.
58. 442 U.S. 735 (1979) has been described by Simmons, *supra* note 43, as a troubling case. The Court held that electronic devices able to capture all phone calls made from a phone line, known as "pen/trap" devices were not a "search" under the Fourth Amendment as the individual had "voluntarily" turned information over to the phone company.
59. 533 U.S. 27, <http://straylight.law.cornell.edu/supct/html/99-8508.ZS.html> (2001), the Court held that a thermal imaging device to scan heat emanating from a suspect's home without a search warrant was a violation of the Fourth Amendment.
60. The Act has effectively extended the "pen/trap" rule of *Smith, supra* note 58, to electronic communications.
61. See Peter Madriñan, "Devil in the Details: constitutional Problems Inherent in the Internet Surveillance Provisions of the USA PATRIOT Act of 2001" (2003) University of Pittsburgh Law Review 783 at p. 804. Investigators must simply certify to a federal magistrate that "pen/trap" surveillance of a suspect's computer communications could gather information likely to be relevant to an ongoing investigation. Their hunch need not be supported with any particular quantum of evidence, but merely state that surveillance is likely to yield information useful to an ongoing criminal or terrorist investigation.

be dissected and manipulated at the convenience of the investigators.

Similarly, the PATRIOT Act has amended FERPA (the act protecting student records). Government officials are able to access student records without court authorization, acting solely on the "good faith" belief that such records are "likely" to contain information related to terrorism.[62] Government access to public, university and college library records has become easier as a result of the PATRIOT Act as well. The minimal requirement that government must meet is that the records are required for an investigation (*N.B.* the patron may not even be an actual suspect). Furthermore, libraries are forbidden under the Act to notify patrons that their records have been requested by government.[63]

For these reasons and others, privacy advocates are unhappy with the PATRIOT Act. The Act opens up great possibilities for prosecutorial misuse and requires only limited judicial oversight. Some opine that the legislation's overall effect has had less to do with terrorism than with easing restrictions on government surveillance of digital communications.[64] Still, it is important to remember that despite the Act's potential reach, it has been rarely put into use—yet. For instance, following repeated requests, the US Attorney General has finally revealed that as of September 2003 the Act had not been used against libraries at all.[65] Furthermore, while the implications of the PATRIOT Act for privacy and its advocates are indeed troubling, it is important for our purposes to remember that they are limited to the role of the public sector. The US Constitution, of course, was never intended to offer protection to Americans from the private sector. As a result, legislative regulation of privacy protection in the private sector has been left to those Acts we summarized above, which apply to specific areas such as health-care, finance and telecommunications. Areas for which there is no specific legislation are protected only by the discipline of the marketplace.

There is of course a great deal of respect in the US (and other countries, we hasten to add) for the powers of the free market. Indeed, one of the emerging themes in the discussion of privacy protection is the extrapolation to the realm of privacy of that well-known libertarian idiom, that the market will always be the most efficient regulator. Privacy regulation through legislation is largely unnecessary when privacy protection is understood in such a manner and privacy advocates would be well advised to sit back and let the market play its part. Government still has a role to play as regulator when the market is responsible for protecting privacy, but it is only to ensure that the market operates as it should. In the context of privacy protection therefore, if private

---

62. Nancy Tribbensee, "Privacy and Security in Higher Education Computing Environments after the USA PATRIOT Act" (2004) 30 Journal of College & University Law 337.

63. Lee Strickland, Mary Minow & Tomas Lipinski, "PATRIOT in the Library: Management Approaches When Demands for Information Are Received from Law Enforcement and Intelligence Agents" (2003) 30 Journal of College & University Law 363, <http://cip.umd.edu/publications/patriot_in_the_library.pdf>.

64. One of the many amendments enacted by the PATRIOT Act converted a "pen/trap" from the passive-surveillance tool that it once was, into a mechanism by which government investigators could expose information revelatory of the intimate details of a person's online activities, before there is probable cause to believe the person is connected with either criminal or terrorist activity. See Madriñan, *supra* note 61 at p. 787. His view is that the current law does not conflate with the underlying principles of the First or Fourth Amendments.

65. Strickland *et al.*, *supra* note 63 at pp. 364-365.

sector bodies have privacy policies, then government's role is merely to ensure that these policies are adhered to. In fact, several Acts that we have discussed above, such as the GLBA, accomplish just that, and the FTC has certainly been actively ensuring that members of the private sector are in compliance with the privacy policies they set for themselves.[66] A respect for the discipline of the marketplace, however, leaves the substance of privacy protection to the market (contrary, as we shall see, to the European and Canadian view).[67]

The debate whether privacy protection is better served in the hands of government or the hands of the market is much broader than the scope of this paper, and is of course part of the larger discussion about the role of government in contemporary society. Interestingly, the US federal government itself has increasingly relied on private sector members for the creation of databases that, if created by government itself, would be subject to the federal *Privacy Act* discussed above. We discuss these activities in greater detail below. It is questionable whether the US federal government has assured itself in such cases that the discipline of the marketplace would ensure the privacy of Americans, or whether it is precisely the absence of legislated privacy protection that has promoted the creation of such databases, respect for the marketplace notwithstanding. Possibly the most significant piece of American legislation supporting our suggestion—that in the US regulation of the private sector is left to the marketplace—is one that we have not included in our summary above: the FTC's proposal for an *Online Privacy Protection Act* (OPPA).[68]

2.1.4. The Online Privacy Protection Act Draft

The Online Privacy Protection Act, sometimes referred to *as The Online Personal Privacy Act*, has not yet been passed by the US Congress. It is not to be confused with California's privacy legislation which bears the same acronym, that has been passed, and which is—due to the size of California's economy—influential on its own as setting privacy standards in the US. California's legislation, the *California Online Privacy Protection Act* (COPPA), is also not to be confused in turn with the legislation protecting children that we have discussed above.

---

66. The most famous recent incident involved pharmaceutical giant Eli Lilly. The FTC has not shied away from publicly exposing members of the private sector that are in violation of their own privacy policies. See FTC, News Release, "Eli Lilly Settles FTC Charges Concerning Security Breach: Company Disclosed E-mail Addresses of 669 Subscribers to its Prozac Reminder Service" (18 January 2002), <http://www.ftc.gov/opa/2002/01/elililly.htm>. Whether the FTC's actions will lead to greater privacy protection or to meaningless privacy policies is open to debate.

67. Canadian privacy advocates have argued that the substantive protections offered by Canadian legislation must be complemented by the public exposure of private sector violations, "FTC-style," in order to be effective. See most recently Michael Geist, "Privacy law perversely protects those who break it" *Toronto Star* (18 October 2004), <http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1098010864947&call_pageid=971794782442&col=Columnist1036500183695> [free registration required].

68. See the latest introduction of OPPA in H.R. 69, 108th Congress, <http://www.nist.gov/hearings/2002/oppa.htm>, 25 April 2002.

OPPA offers a principled and uniform approach to the protection of personal information in the US. The legislation incorporates Fair Information Practice Principles (FIPs) that are comparable to the European principles of privacy protection that we discuss immediately below, and that have been endorsed by the US as early as 1973 (in legislation that we have discussed above, such as the federal Privacy Act).[69] These principles include the requirements for:

1. notice that must be given to a person about use, collection, etc. of personal information;
2. consent that must be obtained from a person in order to collect, use, etc. personal information;
3. providing a person with access to personal information for verification and correction purposes;
4. protecting personal information with the appropriate security; and
5. remedies available to a person to ensure compliance with these FIPs.

OPPA has had the potential of being an effective equivalent to the privacy protection statutes passed both in the EU and in Canada. However, this would-be privacy omnibus Act has languished through several drafts in the US Congress, and the degree of privacy protection offered by it has been watered-down with each successive draft, mainly by changing the scope of the definition of personal information. The current draft, for example, characterizes as personal, information such as a name, address, email address, telephone number and Social Security number. Previous drafts had included additional information as personal, such as health information, financial information, ethnicity, race, political party affiliation and sexual orientation. Such "sensitive" personal information, absent from the current draft, does receive protection under European law, as we shall see below.[70]

The diminished degree of privacy protection offered by the current OPPA draft is understood by us to convey the American faith in the ability of the marketplace to provide such protection. Indeed, taken together with its increased emphasis on ensuring that the private sector is in compliance with the privacy policies it sets for itself, the FTC appears to have abandoned its previous suggestion that the OPPA offers strong privacy protection, with only two of its five commissioners supporting a previous draft in written testimony to the Congressional committee discussing the bill, and the remaining three arguing, in effect, that privacy protection will be obtained through the forces of the

---

69. For a comparison of the FIPs to EU principles see David Baumer, Julia Earp & J.C. Poindexter, "Internet Privacy Law: A Comparison between the United States and the European Union" (2004) 23 Computers and Security 400, <http://www4.ncsu.edu/~baumerdl/C&S_legalComparisonEUvsUS_forJC.doc>.

70. Canadian legislation, perhaps suitable to the middle ground we are advocating, mentions health and financial personal information as "almost always" sensitive, but makes no reference to ethnicity, race, political affiliation or sexual orientation, merely stating that "…any information can be sensitive, depending on the context." See Canada's *Personal Information Protection and Electronic Documents Act*, S.C., 2000 C.5, Sch. I, Principle 4.3.4, <http://laws.justice.gc.ca/en/P-8.6/93196.html> [PIPEDA].

marketplace.[71] There is yet to be a hearing scheduled for the current draft.

The American lack of interest in private sector regulation and the resulting patchwork quilt is one way to approach privacy protection. We attempt to explain this lack of interest by discussing why Americans are primarily concerned about government abuse of personal information. Another approach to privacy protection in the private sector, however, would be to adopt uniform and principled legislation. Accordingly, we now turn to the EU and examine how its legislation protecting personal information developed and evolved to its current state.

2.2. Privacy Regulation in Europe

Europe has proven to be the leader in protecting the privacy of the individual in the digital age. Much of the compilation and transfer of personal information that is a daily occurrence in the US and other countries is illegal in Europe. Some US observers look toward the EU provisions with admiration and hope that Americans will see fit to adopt at least some of the philosophy of protecting consumers against privacy invasions to data, now so commonplace in today's commercial environment.[72] Although we focus on the protection of personal information, it is worth remembering that the EU does not lag behind in the protection of privacy in general, understood as a human right, and expressed as such in the *Convention for the Protection of Human Rights and Fundamental Freedoms*.[73]

2.2.1. Council of Europe

The Council of Europe, established in 1949 in the aftermath of World War II and its horrors, addressed the issue of personal information the very same year.[74] These early efforts led eventually to the *Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data* that was adopted in 1980.[75] The Convention set out basic privacy principles and provided a template for countries without data protection legislation. The principles for automatically processed personal data require that they be:

---

71. For a transcript of that hearing see U.S., *The Online Personal Privacy Act – Full Committee Hearing*, 106th Cong. (2002), <http://commerce.senate.gov/hearings/hearings0202.htm>.

72. See Huie *et al.*, *supra* note 5 at p. 28: "if Directive95/46/EC of the European Union has forced the US government to consider the invasiveness of currently accepted business practice and to enact ameliorative law, then American society, in particular the consumer who alone pitted against business's short-term interests carries little political weight, owes much to the European privacy impetus. It would benefit global society to adopt the philosophy of the directive as the new *ius gentium* for data- privacy law."

73. Art. 8 of the European Convention of Human Rights asserts the "right to respect for private and family life." *Convention for the Protection of Human Rights and Fundamental Freedoms*, 4 November 1950, 213 U.N.T.S. 221 at p. 223, Eur. T.S. 5, <http://conventions.coe.int/treaty/EN/Treaties/Html/005.htm>. We discuss below the common concept at the basis of European legislation on privacy.

74. The Council of Europe was established by ten European countries and was charged with the task of strengthening democracy, human rights and the rule of law throughout its member states.

75. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 28 January 1981, 108 Council Eur. T.S., <http://conventions.coe.int/treaty/en/Treaties/Html/108.htm>. As of December 2001, thirty-three member states had signed and twenty five had ratified this Convention.

1. obtained and processed fairly and lawfully;
2. stored for specific and legitimate purposes;
3. not used in a way that is incompatible with those purposes;
4. adequate, relevant and not excessive in relation to the purpose for which they are stored;
5. accurate, and where necessary, kept up to date;
6. preserved in a form which permits identification of data subjects for no longer than is required for the purpose for which the data are stored;
7. protected by appropriate security measures; and
8. accessible to individuals to enable checking the veracity of the information and enabling correction if necessary.

These principles have been the foundation of subsequent privacy regulation in Europe, and between the EU and other jurisdictions, beginning with guidelines adopted by the Organisation of Economic Co-Operation and Development (OECD) the following year.

2.2.2. *OECD Guidelines*

In 1981, the Organization of Economic Co-Operation and Development, reflecting many of the same concerns with respect to the importance of privacy protection, adopted *Guidelines on the Protection of Personal Privacy and Transborder Flows of Personal Data*.[76] This change was significant as it represented the first trans-Atlantic agreement relating to privacy protection. The *Guidelines* were intended to harmonize national privacy legislation and to provide a framework for facilitating the international flow of data. Eight basic principles were adopted, providing for collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability of the data collector. It is easy to determine that these basic principles mirror the principles established by the European Convention. The *Guidelines* were not binding on OECD members however, and the basic privacy principles increased in legal significance only when the EU Directive on privacy was adopted some seventeen years later.

---

76. *OECD Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 23 September 1980, Eur. T.S. 108, <http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html>.

2.2.3. European Union *Privacy Directive*[77]

The original purpose of the EU *Privacy Directive* was not only to increase data privacy protection within the European Union, but also, as an integral part of EU policy, to promote trade liberalization and ensure that a single integrated market was achieved.[78] The *Privacy Directive* became effective in October of 1998. This Directive covers the processing of all personal data by whatever means, and is not limited by business sector or field of use, although there are exceptions for public security, state security and criminal law.[79] Unlike the US, the EU imposes controls over business processing and use of personal data, both before and after the data are collected. Data controllers are required to inform the data subject of the purpose of the processing and the recipients of the data.[80] The data can be processed and used only for the purposes specified.[81] Some forms of "sensitive" personal information simply cannot be collected (such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health and sex life.) The *Privacy Directive* specifically requires that individuals be informed before personal data is disclosed for the first time to third parties for the purposes of direct marketing, and to be expressly offered the right to object to such disclosures or uses.[82] The *Privacy Directive* further grants individuals the right to challenge any decision significantly affecting them that is based on an automatic processing of data, including decisions involving credit worthiness or employment.[83] Individuals have the right to monitor and challenge the use of personal information after it is processed. The *Privacy Directive* guarantees individuals a permanent right of access to the data about them, to have it corrected and to receive confirmation as to the purposes of the processing and to obtain the identities of third-party recipients.[84] Enforcement is provided for by requiring member states to provide a judicial remedy for infringements of rights.[85] Member states must designate an independent public authority responsible for monitoring the application of the *Privacy Directive* within their territory.[86]

Directives passed by the European Union become law in member states only when legislated by each state's legislature (or passed by some other state administrative institution) and the *Privacy Directive* is no exception. In Italy, for example, the state authority is known as the Garante. The *Privacy Directive* and

---

77. EC, *Council Directive 94/46EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data (Privacy Directive)*, [1995] O.J.L. 281, <http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>.
78. See Shaffer, *supra* note 15 at p.10.
79. *Supra* note 77 at art. 3-2.
80. *Ibid.* at art. 10.
81. *Ibid.* at art. 6.
82. *Ibid.* at art. 14b.
83. *Ibid.* at art. 15.1.
84. *Ibid.* at art. 12.
85. *Ibid.* at art. 22.
86. *Ibid.* at art. 28.

the establishment of the Garante were enabled initially in Italy only by virtue of executive directives issued by the Italian President in a piecemeal fashion, until comprehensive privacy legislation came into force in Italy only in January 2004.[87] Although the format of legislation varies somewhat from member state to member state within the EU, the *Privacy Directive* has been incorporated since 1998 into the laws of every member state.

Not only does the *Privacy Directive* mandate significant regulatory controls over business processing and use of personal data within Europe, it also has significant extra-territorial reach. In article 25, the Directive provides that the EU Commission may ban data transfers to third countries that do not ensure "an adequate level of protection" of data privacy rights. At the time that the *Privacy Directive* was first passed, it presented a serious problem for US companies handling data originating in the EU. Another significant provision for American business is article 26, which lists a number of derogations from article 25. It provides that personal data may be transferred to a country that "does not ensure an adequate level of protection" if the data controller enters into a contract that adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals.[88]

2.3. The US Response to the Privacy Directive: the Safe Harbor Agreement[89]

As discussed above, article 25 of the EU *Privacy Directive* provides that the EU Commission may decide to prohibit all data transfers to a third country if it finds that the third country does not ensure "an adequate level of protection" of data privacy rights.[90] The Safe Harbor Agreement allows onward transfer of EU data to US companies complying with its requirements, and represents acceptance by the EU Commission of the US Department of Commerce's proposed Safe Harbor Privacy Principles relating to US protection of data privacy insofar as they are applicable to European citizens. It is important to note, particularly in the context of this discussion, that the Safe Harbor Agreement is very limited in terms of protecting the privacy of Americans. It applies only to data that originate in the EU and are transmitted to the US to facilitate commerce between them. It was not for the purpose of protecting the privacy of Americans. Safe Harbor recognizes seven privacy principles concerning notice, choice, onward transfer, security, data integrity, access and enforcement. These principles essentially overlap the principles of the European Convention, the OECD and the *Privacy Directive*. Under Safe Harbor, an organization "self-certifies" to the US

---

87. For a summary of privacy law in Italy see Pierluigi Perri & Stephano Zanero, "Lessons Learned from the Italian Law on Privacy – Part I" (2004) 20:4 Computer Law & Security Report 310.

88. *Supra* note 77 at art. 26.2.

89. The Safe Harbor Agreement was released by the EU (EC, *Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and the Council on the adequacy of protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US department of Commerce*, [2000] O.J. L. 215/007, <http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML>) and by the US Department of Commerce on 21 July 2000.

90. *Supra* note 77 at art. 25.

Department of Commerce or to a designated body its adherence to the privacy principles.[91] So far, the industries most represented are information services, computer services and computer software. Noticeably lacking are banks, insurance companies and consumer credit companies,[92] possibly since they must already comply with certain privacy measures under the American privacy legislation that already applies to them, as we discussed above. It is also possible for companies to satisfy EU requirements on a contract-by-contract basis under article 26 of the Directive.[93] Some observers in the US believe that Safe Harbor favours individual privacy too strongly over commercial free speech. These concerns, however, seem to be fading as time has elapsed and affected US companies have adjusted to the cost of handling data originating in the EU. As we shall discuss below, the perceived tension between privacy and the First Amendment may be one of the reasons why Americans have largely shied away from regulating privacy in the private sector.

2.4. Canada's Approach to Privacy

There is no explicit constitutional right to privacy in Canada, although the Canadian *Charter of Rights and Freedoms* contains a right similar to the American Fourth Amendment.[94] The Supreme Court of Canada has noted the critical role of privacy in democracies:

> Society has come to realize that privacy is at the heart of liberty in a modern state….Grounded in a man's physical and moral autonomy, privacy is essential for the well-being of the individual….The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state.[95]

---

91. This is accomplished by a letter, signed by a responsible corporate officer, which contains all contact details, a description of the activities of the organization, the personal information received from the EU, a description of the organization's privacy policy for such information, the date of implementation, the contact person, the specific statutory body that has jurisdiction over the organization, the method of verification (in-house or third-party) and the independent records mechanism that is available to investigate unresolved complaints. The Department of Commerce maintains and publishes a list of all organizations filing such letters.
92. Colin J. Bennett & Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (London: Ashgate Press, 2003) at p. 133.
93. The EU Commission has recently adopted model contractual clauses under art. 26 of the EU *Privacy Directive*. This Article offers the use of these clauses to firms for individual business transactions as an alternative to conformance with the Safe Harbor provision as outlined in art. 25. If used by business on a contract by contract basis, these contractual clauses guaranteeing data privacy will satisfy art. 26 of the 1995 EU Data *Privacy Directive*.
94. S. 8 of the Charter states: "Everyone has the right to be secure against unreasonable search or seizure." See the *Canadian Charter of Rights and Freedoms*, s. 8, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c.11, <http://laws.justice.gc.ca/en/charter/index.html#juridiques>. Unlike the Fourth Amendment, s. 8 is not limited to a physical private domain, and for that reason is considered to provide superior protection. See "Opinion letter from Justice Gérard La Forest to George Radwanski," Privacy Commissioner of Canada (5 April 2002), <http://www.privcom.gc.ca/media/nr-c/opinion_020410_e.asp>.
95. *R. v. Dyment*, [1988] 2 S.C.R. 417, <http://www.lexum.umontreal.ca/csc-scc/en/pub/1988/vol2/html/1988scr2_0417.html> at p. 427 [*Dyment*].

Canada's first major privacy legislation was for the purpose of protecting an individual's privacy in the public sector, *i.e.* from the activities of government.[96] Canada has had a Federal Privacy Commissioner since 1990 whose role it is to monitor violations of private laws and ensure that information gatherers are held accountable. The next significant step in protecting the personal privacy of Canadians was the passage of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) in 1999.[97] This legislation protects the privacy of personal information collected, used or disclosed in the private sector. It does not define personal information, however, except to the extent that it is information that identifies an individual. Canada's motives in passing PIPEDA were twofold. First, it was viewed as a "key lever" in establishing trust and confidence with respect to electronic commerce.[98] In the words of Canada's Minister of Industry at the time:

> By enacting this legislation, the government has put in place a critical element of Canada's Electronic Commerce Strategy….The new law provides the privacy protection that is the foundation of electronic commerce, moving Canada to the forefront of the global digital economy.[99]

The second important reason for this legislation was in reaction to article 25 of the EU *Privacy Directive* and the concern to preserve very important trade relations with the EU. PIPEDA was drafted, therefore, to be compatible with the EU *Privacy Directive*, so that the EU would consider Canada as offering "an adequate level of protection" according to article 25.

Briefly, PIPEDA establishes rules to govern "the collection, use and disclosure of personal information in a manner that balances the right of privacy of all individuals with the need of organizations to collect, use and disclose personal information for a reasonable purpose."[100] The Act has been implemented in three stages: in 2001 it applied to all federal undertakings and all international and inter-provincial trade in personal information; in 2002 it was made applicable to personal information collected, used and disclosed by the health sector; and in 2004 it was made applicable to all organizations that collect, use or disclose personal information during the course of their commercial undertakings, unless the provincial government has implemented substantially similar legislation. As of the present date, in mid 2005, only Quebec,[101] British

---

96. *Privacy Act*, R.S.C. 1985, c. P-21, <http://laws.justice.gc.ca/en/P-21/95414.html>.

97. See PIPEDA, *supra* note 70.

98. Industry Canada, "The Canadian Electronic Commerce Strategy" (22 September 1998), <http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwapj/ecom_eng.pdf/$file/ecom_eng.pdf>.

99. Industry Canada, News Release, "Government of Canada Delivers on Promise to Protect Consumer Privacy" (13 April 2000), <http://www.ic.gc.ca/cmb/welcomeic.nsf/558d636590992942852564880052155b/85256779007b79ee852568c00075c336!OpenDocument>.

100. Industry Canada, "Background Document: Privacy Provisions Highlights," <http://e-om.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/gv00214e.html>.

101. In 1994, the province of Quebec was the first jurisdiction in Canada to regulate the use of personal information by the private sector by passing comprehensive privacy legislation. See *An Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q. c. P-39.1, <http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/P_39_1/P39_1_A.html>. The legislation is based upon the 1980 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, *supra* note 77.

Columbia[102] and Alberta[103] have passed such legislation.[104] Thus, PIPEDA now covers all commercial activity in Canada other than in those provinces where similar legislation is in effect.[105]

PIPEDA has been modeled on the Canadian Standards Association (CSA)'s *Model Code for the Protection of Personal Information* which was developed by business and consumer groups as well as government and was established as a national standard in 1996.[106] The Model Code contained ten privacy principles that have been included in the legislation.[107] They are:

1. Accountability: a designated person must be accountable for an organization's compliance.

2. Identifying Purposes: the purpose for which the information is collected shall be identified at or before the time the information is collected.

3. Consent: the knowledge and consent of the individual are required for the collection, use or disclosure of personal information.

4. Limiting Collection: collection of the information must be limited to that which is necessary for the purposes identified by the organization and information must be collected by fair and lawful means.

5. Limiting Use, Disclosure, and Retention: the information must not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual. Personal information can be retained only as long as necessary to fulfill the purpose for which it was collected.

6. Accuracy: the information must be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. Safeguards: the information shall be protected by safeguards appropriate to the sensitivity of the information.

---

102. The British Columbia *Personal Information Protection Act,* S.B.C. 2003, c. 63, <http://www.qp.gov.bc.ca/statreg/reg/P/PersonalInformation/473_2003.htm>, came into force on 1 January 2004 and has been deemed by the Governor in Council of Canada to be substantially similar to PIPEDA. See *Personal Information Protection and Electronic Documents Act, Organizations in the Province of British Columbia Exemption Order*, C. Gaz. 2004. II. 1640, <http://canadagazette.gc.ca/partII/2004/20041103/html/sor220-e.html>.

103. The Alberta *Personal Information Protection Act*, S.A. 2003, c. P-6.5, <http://canlii.org/ab/laws/sta/p-6.5/20050211/whole.html>, came into force on 1 January 2004, and has been deemed by the Governor in Council of Canada to be substantially similar to PIPEDA. See *Personal Information Protection and Electronic Documents Act, Organizations in the Province of Alberta Exemption Order*, C. Gaz. 2004. II. 1636, <http://canadagazette.gc.ca/partII/2004/20041103/html/sor219-e.html>.

104. British Columbia, Manitoba, Newfoundland and Saskatchewan have passed legislation that covers personal health information.

105. When a province's legislation meets the substantial similarity test, organizations in the province are not subject to the federal private sector privacy law, but must conform to the applicable provincial legislation.

106. Canadian Council for International Business, "Privacy in the Global Economy: Complying with the Requirements of Multiple Jurisdictions" by Matthew Ivis, (Ottawa: Canadian Council for International Business, 2000), <http://www.ccib.org/privacy_in_the_global_economy.htm>.

107. The CSA Model Code was based upon the 1980 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, supra* note 76.

8. Openness: the organization must make specific information about its policies and practices relating to the management of personal information readily available to individuals. Individuals may challenge the accuracy and completeness of the information and have it amended as appropriate.

9. Individual Access: an individual must be informed of the existence, use and disclosure of his or her personal information, given access to it and have the right to challenge its accuracy and have it amended.

10. Challenging Compliance: an individual may bring a challenge to the organization's designated accountable individual alleging a failure of compliance with the principles of the legislation.[108]

As can be seen, the Canadian principles are remarkably similar to the principles outlined in the EU *Privacy Directive*, again, to ensure the EU's recognition of Canada as offering adequate protection of personal information according to article 25 of the EU Directive.

Enforcement of this legislation is the responsibility of the Privacy Commissioner and the Federal Court.[109] The Privacy Commissioner can investigate complaints, mediate disputes, audit compliance, make investigation findings public and appeal to the Federal Court for a remedy.[110] The Federal Court can order companies to comply with the provisions of PIPEDA, to publish notices or correction, and award damages, including punitive damages.[111]

As the foregoing description of Canadian legislation on privacy suggests, Canada and the US have vastly different attitudes and motivations when it comes to protecting privacy, and these attitudes are reflected in the attitudes of Canadian and US companies.[112] This conclusion has been confirmed in a recent cross-national study comparing the corporate privacy practices of comparable Canadian and US firms.[113] The study found that Canadian businesses see their privacy practices as an opportunity to improve relations with customers, while their US counterparts viewed privacy measures more as a way of complying with legislation and avoiding civil lawsuits.[114] The study also found that Canadian companies were more likely to have dedicated privacy officers, resources and training programs.[115] One commentator observed that he thought the study

---

108. Department of Justice Canada, "Privacy Provisions Highlights," <http://canada.justice.gc.ca/en/news/nr/1998/attback2.html>.

109. PIPEDA, *supra* note 70 at ss. 11, 14 and 18.

110. *Ibid.*

111. *Ibid.* at s. 16.

112. See Arthur J. Cockfield, "Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance" 29 Queen's Law Journal 364, <http://www.aals.org/am2002/cockfield.pdf> at p. 370, for an interesting discussion of the different approaches of US and Canadian law to privacy.

113. Study by Ponemon Institutes, commissioned by the Ontario Information and Privacy Commissioner, as reported by Tyler Hamilton in "U.S., Canadian Firms Worlds Apart on Privacy" *The Toronto Star* (24 May 2004) D-1.

114. *Ibid.*

115. *Ibid.*

showed that "the US view of privacy is more a security-centric view,"[116] reflected in US concerns about the PATRIOT Act and the Fourth Amendment, as well as the absence of legislation regulating the private sector. While in Canada, on the other hand, said the commentator, "we have a more European view that says we need to protect against abuse from authorized users,"[117] reflected in the Canadian PIPEDA and the comparable provincial legislation.

*

3. THE CONCEPTUAL BASIS FOR PRIVACY PROTECTION

OBSERVATIONS SUCH AS THE ONE at the end of the section above suggest that privacy is perceived differently, and conceived of differently, in the US, the EU and Canada. In this section we will attempt to substantiate this difference, and through this, to account for the variation in emphasis and regulatory regimes. Beyond the social and economic factors that serve to account for such variations there appears to be a conceptual distinction that leads Americans to question the very need for private sector privacy protection, or, at the very least, the European method of achieving such protection through government regulation. Europeans, in contrast, appear perplexed by what appears to be an American focus on personal information handled by government, at the expense of disregard for private sector privacy practices. Canadians, perhaps because they occupy, as we argue below, a conceptual middle ground, appear to care about both the public and the private sectors' handling of personal information. We argue that perceptions such as whether privacy protection is important in the private sector or not are shaped by conceptions of privacy, and that the US, the EU and Canada do indeed conceptualize privacy differently. We attempt to substantiate our argument below by inquiring into the understanding of privacy as both a social and legal concept in these three jurisdictions. Several attempts have of course already been made to clarify the concept or the idea of privacy, and even to compare the EU and the US.[118] We shall incorporate into these our understanding of privacy in Canada, an understanding that we argue serves Canada well as we occupy the middle ground between the EU and the US.

3.1. The Conceptual Basis for Privacy in the US

Although much has been made in the US of Warren and Brandeis's "The Right to Privacy"[119] as laying the legal foundation for privacy, their argument has not in fact been incorporated into US law. Their call for a privacy right remains, as we mention above, a call yet to be heeded by American lawmakers. It is worth

---

116. *Ibid.*, quoting Peter Hope-Tindall, a privacy consultant in Toronto.

117. *Ibid.*

118. We will focus on Robert C. Post, "Three Concepts of Privacy" (2001) 89 Georgetown Law Journal 2087, <http://www.findarticles.com/p/articles/mi_qa3805/is_200106/ai_n8995411>, and James Q. Whitman, "The Two Western Cultures of Privacy: Dignity versus Liberty" (2004) 113 Yale Law Journal 1151, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=476041>.

119 Warren & Brandeis, *supra* note 6.

remembering in this respect that "The Right to Privacy" focuses most prominently on protection of members of society from the press (we are tempted to call this protection "freedom from the press"), and on achieving this goal through common law and torts. The authors never once mention the US Constitution and its First Amendment, as they apparently, unlike contemporary authors, did not perceive any tension between free speech and the right to privacy.[120] The legislation that has indeed been struck down in the US (the various attempts of Congress to restrict pornography mentioned above, such as CDA, CPPA and COPA) as being against the First Amendment, while ostensibly aiming to protect children from online harm, did not have the protection of privacy as its principal purpose.[121] The legislation that was designed with privacy protection in mind, namely COPPA, has actually been successfully used by the Federal Trade Commission to protect privacy.[122] Furthermore, American case law that has advanced and developed the notion of "commercial free speech" as based on the First Amendment has not done so at the expense of privacy protection.[123] We would even tentatively venture that American case law that does appear to protect privacy at the expense of freedom of expression does not actually revolve around the protection of privacy, but as is the case with legislation such as COPPA, around the protection of members of society from harm.[124]

Although "freedom from the press" is undoubtedly important to certain members of society (Warren and Brandeis used examples of British royalty), other privacy concerns are of much greater import to most of us at present. The increasing concern in the US, as discussed above *vis à vis* the Fourth Amendment

---

120. It is important to remember that the concept of "commercial" free speech had not been addressed by the courts at the time Warren and Brandeis were writing.

121. The latest incarnation of COPA was struck down only recently, in *Ashcroft v. ACLU*, 542 U.S. 656, <http://www.supremecourtus.gov/opinions/03slipopinion.html>, 124 Sup. Ct. 2783, 159 L.Ed.2d 690 (2004).

122. Huie *et al.*, *supra* note 5 at p. 421.

123. The cases mentioned by Huie *et al.*, *ibid.* at pp. 431-434, deal with government regulation of advertisements, not with the exchange of personal information for commercial reasons. In *Bigelow v. Virginia*, 421 U.S. 809, <http://supct.law.cornell.edu/supct/html/historics/USSC_CR_0421_0809_ZS.html> (1975), the State of Virginia regulated advertisements for abortion (advertisements for abortion were illegal) and this regulation was struck down. In *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council*, 425 U.S. 748, <http://straylight.law.cornell.edu/supct/html/historics /USSC_CR_0425_0748_ZS.html> (1976), Virginia's regulation of advertisements about drug prices was struck down (pharmacies were previously not allowed to advertise prices.) In *Bolger v. Young Drug Products Corp.*, 463 U.S. 60, <http://straylight.law.cornell.edu/supct/html/historics/USSC_CR_0463 _0060_ZS.html>, 77 L.Ed.2d 469 (1980), junk-mail about illegal contraceptives was allowed and in *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*, 447 U.S. 557, <http://www.bc.edu/bc_org/avp/cas/comm/free_speech/centralhudson.html> (1980), a utility was allowed to advertise rates. Furthermore, in Central Hudson the court developed a test, where regulation of commercial free speech will only be allowed if the speech is false, or if the government has a "substantial interest" to protect. For a discussion of the test, see Huie *et al.* at pp. 432-434. Nothing here creates the kind of tension that Huie *et al.* believe to exist between the First Amendment and privacy.

124. There are a number of cases dealing with abortion that appear to offer such a protection, all of them building on *Roe v. Wade*, 410 U.S. 113, <http://straylight.law.cornell.edu/supct/html/historics/USSC_CR _0410_0113_ZS.html>, 35 L.Ed.2d 147 (1973) [*Roe*]. To us, it would seem these cases indeed protect women from harm, but do not necessarily seek to protect women's privacy. For example, this is seen in *Hill v. Colorado*, 530 U.S. 703, <http://supct.law.cornell.edu/supct/html/98-1856.ZS.html>, 147 L.Ed.2d 597 (2000), where the rights of protesters to free speech were curtailed by the rights of women seeking abortion to be let alone. We do not believe a convincing analogy can be drawn between the rights of these women and the rights, yet to be established in the US, of members of society with respect to their personal data held by the private sector, although others would disagree. See Huie *et al.*, *ibid.* at pp. 436-441.

and the PATRIOT Act, relates to government intrusion into the private lives of Americans.[125] We must recognize, however, that this use of the phrase "the right to be let alone" is not its use as intended by Warren and Brandeis.[126] They thought of the right to be let alone by the press, not, as some might assume today, by government. By way of extrapolation we will argue below that today they would have thought of "the right to be let alone" by the private sector.[127] At the same time, American understanding of "the right to be let alone" has shifted and has come to stand for an American desire for as little government intrusion as possible. The conceptual basis that has enabled this shift is the understanding of privacy as based on the idea of liberty.[128]

A theory of privacy as liberty envisions the protection of privacy as the protection of liberty. Privacy is important inasmuch as it protects the liberty that is its foundation, and there is no reason and no need to protect privacy if liberty is not in danger. The idea that privacy protection flows directly from liberty protection is the key to our understanding of American privacy law. In *Whalen v. Roe*, mentioned above, the Supreme Court endorsed three distinct privacy interests:

> The concept of a constitutional right of privacy still remains largely undefined. There are at least three facets that have been partially revealed, but their form and shape remain to be fully ascertained. The first is the right of the individual to be free in his private affairs from governmental surveillance and intrusion. The second is the right of an individual not to have his private affairs made public by the government. The third is the right of an individual to be free in action, thought, experience, and belief from governmental compulsion…. The first of the facets…is directly protected by the Fourth Amendment; the second and third correspond to the two kinds of interests [protected by the Fourteenth Amendment].[129]

The Fourteenth Amendment does not discuss privacy directly. The privacy interests mentioned by the court are protected by Section 1 of the Fourteenth Amendment, which states:

> No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.[130]

---

125. For example, Post, *supra* note 118 at pp. 2094-2095; Whitman, *supra* note 118 at pp. 1161-1162.
126. Warren and Brandeis, *supra* note 6 at p. 193.
127. Interestingly, Post believes protection from the press not to be a form of privacy protection at all. See Post, *supra* note 118 at p. 2090.
128. Post, *ibid.* at pp. 2095-2098.
129. Philip Kurland, "The Private I" (1976) 7 University of Chicago Magazine 8, reprinted in *Whalen, supra* note 11 at p. 599, referring to footnote 24.
130. U.S. Const. amend. XIV, s. 1, <http://www.yale.edu/lawweb/avalon/usconst.htm>.

Although the "due process" protection of the Fourteenth Amendment was understood at first to be procedural, the Supreme Court has come to interpret it as offering substantive protection as well. One of the rights that the Court has understood to be protected by the idea of substantive due process has been the right to privacy.[131] Since in *Whalen v. Roe* the issue was the applicability of the Fourteenth Amendment the Court went on to elaborate the second and third interests:

> One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions.[132]

Now these three interests or facets quoted above can roughly be understood as anonymity, secrecy and autonomy. There are two points we wish to make about them. The first is that there is of course a great deal of overlap between these privacy interests in the daily lives of members of society. For example, the Supreme Court takes anonymity to be protected by the Fourth Amendment but that is correct only to the extent that an individual's activities are conducted in the "private" sphere, where an individual has reasonable expectations of privacy to begin with. Attempts to extend Fourth Amendment protection into the "public" sphere explicitly for the purpose of preserving anonymity, as in the example of video surveillance of public spaces, have been rejected by the Court,[133] even though anonymity has at times been explicitly defined as "privacy in public," meaning "a 'state of privacy' that occurs when the individual is in public places but still seeks and finds freedom from identification."[134] So arguably, the Fourth Amendment, at least as it is currently understood by the Court, serves to protect secrecy more than anonymity.[135] The second point we wish to make is that there are two ways of interpreting the Court's comments on privacy. In the first quotation above it is clear that privacy is a right that deserves protection from government. Anonymity is anonymity from government, secrecy is secrecy from government, and most importantly perhaps for our purposes, autonomy is autonomy from government. Whatever the privacy interest, they are all protected from government. Since as we have just seen privacy interests tend to overlap it does make sense that the Court will emphasize their common aspect, that is, the protection of an individual from the long reach of government. Essentially, therefore, protection of one's privacy is protection of

---

131. That was the Court's reasoning in *Roe*, *supra* note 124, and earlier, in *Griswold v. Connecticut,* 381 U.S. 479, <http://supct.law.cornell.edu/supct/html/historics/USSC_CR_0381_0479_ZO.html> (1965).

132. *Whalen*, *supra* note 11.

133. See Blitz, *supra* note 40.

134. Alan Westin, *Privacy and Freedom* (New York: The Association of the Bar of the City of New York, 1967) at p. 31.

135. The Court did leave the door open to the application of the Fourth Amendment to public spaces in the event of "dragnet" searches, in *United States v. Knotts*, 460 U.S. 276, <http://www.justia.us/us/460/276/index.html> (1983). This open door has led privacy advocates to argue that the advent of CCTV and GPS technology is in effect a "dragnet" as envisioned by the court. See Slobogin, *supra* note 47 at pp. 219-222.

one's liberty, and privacy itself is understood as the way in which individuals resist the coercive, standardizing power of the state.[136] However, there is another way to interpret the Supreme Court's position. In its further elaboration of the privacy interests protected by the Fourteenth Amendment (the second quotation above) the Court makes no explicit reference to government. Hence, we are free to envision that privacy means for individuals not only shielding their activities from the prying eyes of government, but from their neighbours as well, and that individuals would like to have control over their personal affairs whether the party attempting to seize control from them is government or a private business. Once privacy is understood in such a manner, however, then it is clear that privacy may protect more than an individual's liberty. Privacy may protect an individual's social standing, or dignity, as well.[137] The conception of privacy as protecting dignity has been used to argue against Closed Circuit Television (CCTV), for example, although we discuss below whether government video surveillance is an offence to dignity according to our understanding of it as a conceptual basis for privacy.[138]

From our examination of US privacy legislation and the legislation that indirectly addresses privacy concerns, it seems to us that in the US privacy is on the whole taken to protect liberty more than dignity. The *Privacy Act*, *Privacy Protection Act*, *Driver's Privacy Protection Act*, *Right to Financial Privacy Act*, ECPA, and FERPA, are all concerned with protecting personal information from falling into the hands of government, or if already in the hands of government, from abuse. The Fourth Amendment is important to privacy advocates in the US because it protects American freedoms from the long arm of government. The PATRIOT Act is such a threat to privacy since it is ultimately a threat to the liberties Americans enjoy.[139] The concerns over video surveillance and DNA databases all have to do with protecting an individual from government. Protection from government is of course the protection of liberty, and therefore warranted. But protection of personal information in the hands of the private sector from potential abuse appears to be unwarranted since the private sector does not endanger liberty, but is at most a nuisance to the American at dinnertime.[140] Telephone and cable companies are prevented from soliciting further business from their customers under the *Cable Communications Policy Act* and *Telecommunications Act* and so one dinnertime nuisance is eliminated. Another nuisance, the telemarketer, is prevented from calling potential customers under the *Telephone Consumer Protection Act*. Meanwhile, personal

136. For more on this conception of privacy, see *supra* note 6.

137. We should stress that this is not the Supreme Court's position. In *Whalen*, *supra* note 11, the Court endorsed the earlier finding of *Roe*, *supra* note 126, and stated: "the 'right of privacy' is founded in the Fourteenth Amendment's concept of personal liberty" at footnote 25 of *Whalen* at p. 598.

138. For the argument against CCTV based on dignity see Slobogin, *supra* note 47 at p. 284.

139. Furthermore, the reasons offered by the American government for the PATRIOT Act show that the Administration understands privacy precisely as the freedom from government as well, and justifies such legislation as an unwelcome but necessary intrusion of government on the American people's privacy in these troubled times.

140. Related to this apparent "trust" of the private sector is the absence in the United States of a general presumption that data should be used only for the purpose for which they are collected, whereas this principle is important in Canada and the EU. See Swire & Litan, *supra* note 15 at p. 178.

credit information can be exchanged among businesses freely, as long as it is done fairly, since that is all that the FCRA stipulates and since such a free exchange will result in a fair interest rate for customers.[141] Financial institutions must have privacy policies, but these policies may reveal that the institutions will not protect personal information at all, since there are no guiding principles for them in the GLBA. American employers may survey employees both physically and electronically with impunity, and American businesses may similarly survey their customers, since such surveillance is conducted on the employer's or business's property or in public, where the courts have found that Americans do not have an expectation of privacy.[142] Americans, however, can rest assured that no one will know what videotapes they have borrowed without their consent, thanks to Judge Bork and the *Videotape Privacy Protection Act*.

Most significantly perhaps, when the private and public sectors work hand in hand, as seems to be the case with federal agencies and Commercial Data Brokers (where the private sector compiles massive databases for public sector access ostensibly for law-enforcement purposes), Americans express very little outrage at the fact that their personal information is in the hands of a business.[143] Americans are concerned, it would seem, about Commercial Data Brokers only since these companies permit government access to their databases. It is the government access which worries Americans, not the existence of the databases themselves, while citizens of other countries have expressed outrage that such databases exist to begin with.[144] Such American concerns indicate to us that the American conception of privacy is primarily based on the protection of liberty, rather than dignity.

Furthermore, where some legislation attempting a more principled approach to privacy protection in the private sector is in place, such as COPPA (protecting children's personal information) or HIPAA (protecting medical personal information), an alternative justification for its conceptual basis is made. COPPA, for example, is perceived as protecting children from harm, and not as primarily protecting their privacy, since the children are protected not from government, but from other members of society.[145] When justification for HIPAA

---

141. See Oliver Ireland & Rachel Howell, "The Fear Factor: Privacy, Fear, and the Changing Hegemony of the American People and the Right to Privacy" (2004) 29 North Carolina Journal of International Law & Comparative Regulation 671.

142. American airlines, such as JetBlue, are now installing CCTV in passenger cabins, yet private sector surveillance appears of little concern to American privacy advocates. See Roberto Iraola, "Lights, Camera, Action! – Surveillance Cameras, Facial Recognition Systems and the Constitution" (2003) 49 Loyola Law Review 773. Ironically, when the tables were turned on the judiciary, and software monitoring internet usage was installed on the computers of members of the 9th Circuit, no time was lost by the court in demanding its removal. See Andrew Taslitz, "The Fourth Amendment in the Twenty-First Century: Technology, Privacy and Human Emotions" (2002) 65 Law & Contemporary Problems 125, <http://www.law.duke.edu/shell/cite.pl?65+Law+&+Contemp.+Probs.+125+(Spring+2002)> at p. 128.

143. See Hoofnagle, *supra* note 18; Dempsey, *supra* note 18.

144. The uproar was primarily in Latin American countries where American Commercial Data Brokers operated. See Hoofnagle, *ibid*. at pp. 612-616.

145. Which is why, confusing acronyms not withstanding, it is often conflated in discussions with other child-protecting legislation, such as the child pornography acts that have been stricken down by the Supreme Court of COPA (most recently) and its predecessors CDA and CPPA.

is sought, then the Supreme Court's articulation of privacy as "the interest in independence in making certain kinds of important decisions" in *Whalen v. Roe* is sometimes referred to.[146] Independence in such a context, we argue, is more closely related to the conception of privacy as dignity, autonomy, and maintaining personal control, than it is to the protection of the individual from government. It can be argued of course that it is ultimately an empirical question whether Americans understand privacy protection as liberty protection, and the evidence we can offer in support is anecdotal at best.[147] It is telling that what little regulation of the private sector that exists in the US is understood by Americans themselves to be conceptually distinct from the pervasive American attempts to restrain government. To date, any attempt to pass principled legislation protecting personal information in the US private sector has remained in draft form (*i.e.* OPPA), no matter how minimal the protection. The concept of privacy governing Americans, it seems, is privacy as liberty.

3.2. The Conceptual Basis for Privacy in the EU

The distrust of government, and the formulation of privacy as the legal response to this distrust, seem unique to the US, at least when compared to the EU (more on Canada momentarily). But if citizens of the EU are less inclined to view their government as unnecessarily intrusive then what are their privacy concerns about? We have already hinted at this alternative above, and to support our suggestion as to the answer to this question, we revisit the "right to be let alone." Warren and Brandeis perceived in British royalty a desire not to be subject to the scrutiny of the press, a scrutiny that would result in unnecessary humiliation. It is the desire to avoid humiliation that seems to be the driving force behind privacy legislation in Europe. This is a conception of privacy protection as dignity, rather than liberty, protection.[148]

Dignity protection is conceptually distinct from liberty protection. "Liberty" is a political value. "Dignity" is a social concept. To protect dignity is to protect a certain social status, a certain image of one that society holds. The protection of dignity consequently is the enforcement of certain relevant social norms.[149] Dignity is protected first and foremost in society, so one's dignity does not necessarily suffer from government actions as much as it potentially suffers from the thoughts and perceptions of other members of society. If the goal of

146. See Tamela White & Charlotte A. Hoffman, "The Privacy Standards under the Health Insurance Portability and Accountability Act: A Practical Guide to Promote Order and Avoid Potential Chaos" (2004) 106 West Virginia Law Review 709. There is no caselaw on HIPAA as of the summer of 2004 and some argue that little will change under HIPAA. See Joan Kiel, "The Health Insurance Portability and Accountability Act (HIPAA) Implementation via Case Law" (2004) 20 Journal of Contemporary Health Law & Policy 435.

147. For example, advocates for abortion, and for the right to bear arms both support their position by using privacy protection arguments. But are the right-to-choose and the-right-to-bear-arms important privacy rights, or is it the heart of the matter that they are liberties that some Americans believe must not be infringed upon by government?

148. Post, *supra* note 118 at pp. 2092-2093.

149. This status, and these norms, may vary of course from one society to another.

privacy protection is ultimately the protection of dignity, then it is clear that privacy must be protected first and foremost in society, and that government intrusions are less worrisome. To some degree of course, an erosion of liberties will result ultimately in the erosion of dignity, and to that extent government intrusions will be worrisome even for those concerned primarily with the protection of dignity. Certainly for Europeans, having suffered abuse at the hands of totalitarian governments through World War II and the ensuing Cold War, such concerns are never far from their mind. But for societies concerned with dignity the activities within society are potentially more problematic than the activities of the governing regime. Concerns about social activities are not limited of course to Warren and Brandeis's pesky press harassing British royalty. Plebeians too can worry about their dignity, as it is reflected in the way they are treated by their employer, their neighbours, or by businesses with whom they interact.

The extent to which the attitude of European citizens towards privacy is based on their desire to preserve their dignity is an open question of fact, and there are of course distinctions between the member states themselves, and even within member states.[150] For instance, privacy is understood differently within Great Britain, by England and Scotland. Although in terms of personal information both England and Scotland are subject to the same Data Protection Act which implements the EU *Privacy Directive*, and both England and Scotland are subject to the same *Human Rights Act*, which implements the *European Convention of Human Rights* and article 8 in particular,[151] the two jurisdictions do have their differing opinions. English courts have rejected the idea, for example, that article 8 creates a tort in privacy, or that it offers protection to individuals from other individuals (known as horizontal protection.) Instead, English courts have viewed the *Human Rights Act* as protecting individuals from government (vertical protection), and have understood privacy as a "freedom," similar to the American understanding of liberty.[152] Scottish courts, on the other hand, have awarded damages for both "the invasion of privacy and liberty," and although there is presently no Scottish case law based on the *Human Rights Act,* it appears the Scottish courts are prepared to apply article 8 to protect individuals from others, not only from government.[153]

Although Scotland and England have their differences as to the scope of protection granted to individuals under the *Human Rights Act*, when protection of an individual from government was the case both English and Scottish courts tied privacy and liberty together.[154] The understanding of privacy protection as liberty protection, we have argued, is the American conception of privacy, and it

150. In addition, we cannot be certain to what extent to which this is an attitude not shared by Americans or Canadians. Excellent work has already been done comparing the US and the EU by Whitman, *supra* note 118, who indeed argues that the EU concept of privacy is based on dignity, whereas the US concept of privacy is based on liberty.

151. Art. 8 creates the "right to respect for private and family life."

152. See Jonathan Morgan, "Privacy Torts: Out with the Old, Out with the New" (2004) 120 Law Quarterly Review 393.

153. See Hector MacQueen, "Protecting Privacy" (2004) 8 Edinburgh Law Review 248.

is clear from the British example that it is not foreign to European jurisprudence.[155] Still, it is not the prevalent conception of privacy in Europe. Turning to Great Britain again, when privacy from other individuals is contemplated, Scottish discussion attempts to base privacy on dignity, as does the English understanding of the *Data Protection Act*.[156] Despite the differences, therefore, within British jurisprudence that we have brought forward as an example, and within Europe more generally, we argue that the conception of privacy as dignity explains much about the Europeans' aggressive position on private sector regulation (as well as their relative lack of concern over government intrusion). This is illustrated on the one hand by acceptance in Great Britain of government video surveillance that amounts to an "electronic dragnet" in American eyes and by a blasé European attitude towards government-required identity cards, as they do not perceive them as damaging their dignity.[157] On the other hand employment law cases in which European courts have affirmed that employers have very limited rights of surveillance over employees serve to protect the dignity of employees.[158] Consider now the European principles of personal data control, such as the requirement for informed consent, the right to correct the data and monitor their usage and the right to challenge any significant decision made on the basis of the data. These rights and principles guarantee the dignity of the individuals to whom the data belong. There is no protection here of privacy as liberty, no concern over the role of government. What these principles do offer is protection of the public persona European citizens perceive themselves to have, protection of their image as they would like others to see it.

Finally, the importance of dignity as a value to Europeans does not have to be indirectly inferred from privacy principles, anecdotal evidence, or the values of other jurisdictions.[159] It is front and center in Europe's future Constitution. The current version of the European Constitution states that the EU is founded on the value of human dignity,[160] that the EU's *Charter of Rights* is founded on the value of human dignity,[161] and devotes an entire Title within that Charter to dignity.[162] Once the Constitution is adopted by European member states the conception of privacy as dignity will only be strengthened.[163]

---

154. For example, the English case, *Wainright v. Home Office*, [2003] 3 W.L.R. 1137, 4 All E.R. 969 (HL), and the Scottish case, *Henderson v. (Moodie) Chief Constable of Fife*, [1988] S.L.T. 361.
155. Surveys have shown, however, that on the whole Britons trust their government more than Americans trust their government. See Taslitz, *supra* note 142 at pp. 172-173.
156. MacQueen, *supra* note 153.
157. On CCTV in Britain. See Slobogin, *supra* note 47 at pp. 222-223.
158. For a discussion of these cases, see Whitman, *supra* note 118 at pp. 1194-1196.
159. For example, South Africa, whose Constitution bases the rights it provides for on the fundamental value of human dignity in Section 1. The South African Constitution has been touted as model for Scottish law. See MacQueen, *supra* note 153.
160. Part II, art. 2. For the current version see <http://europa.eu.int/eur-lex/lex/en/treaties/dat/12004V/htm/12004V.html>.
161. Preamble to Part II.
162. Part II, Title I. The European Charter also includes a right to "respect for private and family life" in Article II-7, and a right to "protection of personal data" in art. II-8.
163. Europeans accept government intervention as necessary for dignity protection in other areas as well, such as the regulation of forenames and surnames. Americans find the very idea incomprehensible. See Whitman, *supra* note 118 at pp. 1215-1219.

3.3. The Conceptual Basis for Privacy in the Canada

While it is the conception of privacy as dignity that facilitates government intervention and regulation as the EU directive requires, it is the conception of privacy as liberty that prevents Americans from contemplating this sort of government regulation. We now ask, if Americans understand privacy as the social and legal construct that protects their liberty and Europeans understand privacy as the social and legal construct that protects their dignity, then what is the middle ground occupied by Canadians? We begin to construct this middle ground with the reiteration that privacy is not based exclusively on liberty for Americans, nor is it based exclusively on dignity for Europeans. This is a truism recognized already by Warren and Brandeis.[164] Americans, and Europeans, are at times more concerned about their liberty, at times more concerned about their dignity, and at times concerned how their (lack of) liberty will affect their dignity.[165] All we have argued is first, that the concepts of liberty and dignity are distinct, since liberty is at the basis of an individual's relationship with government, and dignity is at the basis of an individual's relationship with other members of society. Second, that on the whole, American privacy law better reflects a value of privacy as liberty, and that on the whole European privacy law better reflects a value of privacy as dignity. We now wish to argue that despite these differences a middle ground can be found, and it can be found in the concept of autonomy, in the individual's sense of control.

As concepts "liberty" and "dignity" may seem distinct, yet they can both be understood as manifestations of autonomy, one in the political arena, the other in the social field. Autonomy, therefore, is actually better understood not as a facet of privacy as the US Supreme Court contemplated in *Whalen v. Roe*, alongside anonymity and secrecy, but as a fundamental value of human life in contemporary society. Precisely what is controlled by the individual changes of course from society to society. When Americans fiercely protect their liberty they are showing their government who is really in control. In America one's home is one's castle not in the traditional British sense of a sanctuary from the prying public, but in a new sense of sovereignty, a sphere over which no one else has control. Americans care more about controlling government—it must be put, and kept, in place and never allowed to think itself more important than the members of society it attempts to govern. So Americans will not accept government telling them what to name themselves or their children, or telling them what they can and cannot do with information they have obtained. On the other hand, Americans accept without question government's authority in naming public places such as towns or roads, or legal persons such as corporations.[166] Why? Because Americans feel government activity in such spheres does not ultimately infringe on their control of their political role.

---

164. As well as by Post, *supra* note 118 at pp. 2095-2096, and Whitman, *supra* note 118 at pp. 1162-1164.
165. For example, the European concern that the more totalitarian a regime, the less dignity within society.
166. For example, the State of Maine prohibits offensive public names containing "nigger" or "squaw." Practically all US jurisdictions prohibit incorporation of offensive names.

Similarly, Europeans proudly protect their dignity—they are showing their corporations who is really in control. Europeans care more about controlling the perceptions of society, their public image. That is why they allow government to forbid certain names, and that is why Europeans object so strongly to any of their personal information being disseminated without their permission, without their control.

So it goes without saying that different societies have different approaches to autonomy and the social and political spheres where it is manifested.[167] Where is Canada located on this scale? As we already implied—in the safe middle ground.[168] The Supreme Court of Canada has identified three zones of privacy—or as we put it, areas of autonomy—over which, it is presumed, members of society exercise control: personal space, dignity, and personal information.[169] Privacy of one's personal space builds on the notion of liberty protection. Here Canada's privacy protection, stated in Section 8 of the *Canadian Charter of Rights and Freedoms* as we discussed above, resembles the American protection as enshrined in the American Fourth Amendment. Protection of dignity resembles of course the European notion of privacy protection. Of the three areas of privacy autonomy, the protection of personal information is where we see Canada serving as a middle ground. As discussed above, Canada has had in place legislation to protect personal information in the hands of government and other public bodies for some time,[170] as well as legislation to protect personal information in the private sector (PIPEDA). We believe Canadians are concerned as to the manner in which their personal information is handled once it is out of their hands, not only because this represents a threat to their liberty if it is mishandled by the public sector, or a threat to their dignity if it is mishandled by the private sector, but also because Canadians do not want to lose their autonomy, their control over this information, which is, after all, personal.

Indeed, the Federal Privacy Commissioner of Canada, established to supervise the use of personal information in Canada, offers the following understanding of privacy:

> ...the right to control access to one's person and information about one's self. The right to privacy means that individuals get to decide what and how much information to give up, to whom it is given, and for what uses.

Most Canadians appear to share the Privacy Commissioner's definition of privacy. Privacy to them is about control—the right to control one's personal

---

167. Consider again autonomy as liberty. Not only is there a distinction between Europe and the US, but Europe itself is of course not uniform in its attitude to government, with the Germans arguably at the more authority-respecting end of the spectrum, through the British with their trust in their "good government" somewhere in the middle, and finally with, say, the Italians at the less respectful end.

168. For more on Western democracies and autonomy within them, see Bennett, *supra* note 92 at pp. 14-15. Bennett does not offer a unique Canadian concept of privacy in terms of autonomy.

169. *Dyment*, *supra* note 97. For a discussion, see Elizabeth F. Judge, Book Review of *The Law of Privacy in Canada* by Barbara McIsaac, Rick Shields & Kris Klein, (2000) 32 Ottawa Law Review 311 (2000) at pp. 313-315.

170. Canada's *Privacy Act* was enacted in 1982. See *supra* note 96.

171. Treasury Board of Canada, "So, What Exactly is Privacy?" <http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/course1/mod1/mod1-2_e.asp>.

information and the right to choose to remain anonymous.[171]

We believe that Canada is well positioned to become a bridge between Europe and the US for other well known reasons as well. Canada has much in common with the US in terms of history (we are both former colonies); its geography (we are both massive North American countries with rich natural resources); and political structure (we are both federal countries with powerful and difficult state and provincial sub-sets). In many ways Canada resembles the US more closely than the EU. Western Canada, in particular is partial to the American emphasis on personal liberty. Yet Canada is also deeply connected to Great Britain and France, and is in the process of a long multicultural political experience drawing on diverse cultures from five continents. Thus Canadians, like Americans, do not accept government intervention into the naming of children, yet are willing to tolerate government restrictions on corporate and other public names.[172] Canadians, like Americans, are concerned about DNA databases and public video surveillance.[173] On the other hand, Canadians, as do Europeans, expect certain dignity from the private sector and in the workplace. Our trade-unions have recently taken a case of workplace surveillance to the Federal Court of Canada.[174] Canadians have also appeared to reject the idea of national identity cards, yet it is interesting to note that, unlike Americans, whose attitudes were very negative, in Canada there was a lively political discussion, with substantial political support given to the idea.[175]

It is Canada's coalescing identity as a multicultural haven that we perceive is the foundation of Canada's conception of privacy as autonomy protection. One of the fundamental values of a multicultural society—as opposed to either a traditionally homogenous society or a "melting-pot" society—is tolerance and respect for other members of society's autonomy and control of both their social, and political, personae. A multicultural society does not attempt to impose on its members values, which some elements in it may very well hold dear—such as dignity or liberty—but encourages the development of these values autonomously, within a multicultural framework. Canadians, it seems, perceive their privacy as most importantly protecting this autonomy, and believe that members of society should be free to decide for themselves what is important for them to control.[176]

---

172. The province of Alberta's legislation, for example, states: "No corporation or extra-provincial corporation registered in Alberta may have a name that contains either of the following: a word or expression in any language, that is obscene or connotes a business that is scandalous, obscene or immoral or that is otherwise objectionable on public grounds. See *Business Corporations Act,* R.S.A. 2000, c.B-9, <http://www.canlii.org/ab/laws/regu/2000r.118/20050110/whole.html>.

173. Several provincial privacy commissioners have published guidelines for the use of CCTV in both public and the private sectors. For Ontario's guidelines see Ontario, Information and Privacy Commissioner, *Guidelines for Using Video Surveillance Cameras in Public Places* (Toronto: Information and Privacy Commission, 2001) (Commissioner: Ann Cavoukian), <http://www.ipc.on.ca/docs/video-e.pdf>.

174. The Federal Privacy Commissioner's findings that prompted the case are available at <http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040219_02_e.asp>.

175. A summary of the debate is available from Canada's Privacy Commissioner available at <http://www.privcom.gc.ca/keyIssues/ki-qc/mc-ki-nid_e.asp>.

176. The important issue of our day and age would seem to be personal information.

*

4. CONCLUSION

AMERICANS, AS WE HAVE SAID, value their liberty. Americans want their government to let them interact freely with one another and to not intervene. This is the conceptual underpinning of the current state of privacy protection legislation in the US. If government only leaves the marketplace alone, Americans seem to believe, it will take care of itself. We question whether this remains the prevailing attitude. There have been many concerns raised in the US about the latest government intrusions into privacy in the form of the PATRIOT Act, but there have also been concerns raised about the lack of protection from private sector electronic surveillance and data collection to the extent that Americans are willing to rethink the employment relationship and its implications for privacy:

> Surely this… vision of the modern workplace rooted in principles of industrial organization from the 1920s is hard to accept today. As e-mails, modems, and PCs break down the boundaries between work and home, there are progressively fewer private or public spaces for citizens to express themselves autonomously. The Internet has blurred the distinction between the home and the office, as Americans are spending more time at the office and are using company-owned computers and Internet servers to do their work from home. But as technology poses new challenges to geographic concepts of privacy, courts have not been encouraged to think creatively about how to reconstruct zones of individual privacy and free expression.[177]

One way of thinking creatively about privacy, according to American privacy advocates, is the European way. European privacy law is viewed as the "last, best hope" for the extension of private sector privacy protection to Americans, and privacy advocates in the US have called for the US to follow and emulate Europe.[178] So far the US has not shown any intention of moving to create omnibus legislation, a comprehensive regulatory authority or an American "Privacy Czar," similar to authorities and legislation already existing in European countries and in Canada. Our argument has been that economic forces will probably not suffice to bring about this change in the US, as the difference in approach between the US and Europe rests on deeper conceptual differences as we have discussed. The concept of liberty is ingrained into American society in much the same way as dignity is entrenched in European societies. It is difficult to conceive that privacy protection could rest on a different foundation in the US, although as we have seen in the case of HIPAA such alternative foundations are at the very least contemplated. We believe an alternative foundation is possible, based on the idea of autonomy and personal control as is emphasized in Canada.

---

177. Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (New York: Random House, 2000) at pp. 83-84.

178. For example, Huie *et al.*, *supra* note 5 at p. 423; Reidenberg, *supra* note 5 at p. 746.

Consider nudity, not necessarily as a lifestyle change but as an example of privacy protection.[179] Americans feel they lose their privacy when they are nude. Nudity serves as a metaphor in American discourse for other situations in which privacy is lost.[180] Although it is difficult for Americans to comprehend that a person can be physically naked, yet feel no loss of privacy, this understanding of privacy does not rest on its conception as liberty. Significantly, and perhaps somewhat counter-intuitively, it does not rest on a conception of privacy as dignity either. Indeed, Europeans would not easily understand the metaphorical use of nudity as signifying privacy loss since many Europeans happily go nude in public without feeling any loss of privacy or any loss of dignity.[181] We suggest the American perception of nudity, as a situation without privacy, is based not on liberty and not on dignity, but on personal control or autonomy. Americans feel they are not in control over their person when they are nude, while Europeans feel very much in control. Significantly, Canadians—perhaps even more than Americans—do not disrobe with ease and feel they lose their privacy if naked, precisely because personal control is the significant value underpinning privacy for Canadians.[182]

The nudity example is but an anecdote, yet it serves as a reminder that alternative conceptions of privacy co-exist in the US. The following for example is an American, and not, as could perhaps be expected, a Canadian conception of privacy:

> Privacy as a legal right can be described as, on one hand, the right of the individual citizen to be secured against unlawful or unwarranted surveillance; and on the other hand, as the right of the individual to control access to personally identifiable information.[183]

We believe Americans must build upon these alternative conceptions, and most significantly on the idea of privacy protection as an exercise in autonomy, if they are to seize the initiative and extend privacy protection to the private sector. After all, personal control of information and protection of this information from abuse by the private sector were called for by Warren and Brandeis over a century ago. It is time for Americans to remember that the "right to be let alone" should apply not only to government, but to the private sector as well. There is no better reminder than a renewed emphasis on the value of autonomy as a Canadian middle ground that Americans are welcome to join.

---

179. See Whitman, *supra* note 118 at pp. 1200-1202"

180. For example, "persons caught in the 'pitiless glare' of public attention typically feel naked and demeaned" because they lose their privacy. Post, *supra* note 118 at p. 2093.

181. Whitman, *supra* note 118 at p. 1201.

182. Canadian nudists in British Columbia have complained in the summer of 2004 that two high-rise student dormitories built by the University of British Columbia overlook their nudist beach, and that as a result they will lose their privacy. Clearly privacy for the nudists is understood as their power to control who views their naked bodies, rather than feeling ashamed of being naked to begin with.

183. Herman Tavani, "Privacy and Security" in Duncan Langford, ed., *Internet Ethics* (New York: Macmillan, 2000) 65-95 at pp. 66-67.