Protecting Privacy and Enabling Pharmaceutical Sales on the Internet: A Comparative Analysis of the United States and Canada

Nicole A. Rothstein*

* Candidate for J.D., Georgetown University Law Center, May 2001. The Author wishes to thank Professor Angela J. Campbell for her guidance in writing this piece.

I. INTRODUCTION

The Internet offers the potential to revolutionize the manner in which people receive health information and treat their health conditions. More than 40.9 million Americans were expected to use the Internet in the year 2000 for health care.[1] "According to *Investors Business Daily*, 43 percent of [W]eb surfers access health care data online each year. Health concerns are the sixth most common reason that people use the Internet, and according to the market research firm, Cyber Dialogue Inc., this number is growing by 70 percent a year."[2]

Even without the growth of the Internet, the twentieth century has seen an incredible proliferation of health care services. Rather than simply consulting a single family physician for all health-related matters, patients now seek counsel from many individuals about needed services. The Internet offers an easy, fast, and potentially more robust source of health care delivery. Nonetheless, this incredible new medium also has the potential to defraud consumers seeking health information and services in a manner that probably would not have occurred had they simply consulted their familiar—and trusted—licensed medical practitioners.

Generally, the health care industry has lagged behind other sectors in the use of information technology services and solutions.[3] In the modern health care arena, however, sharing information is increasingly important to facilitate patient diagnosis and treatment, insurance and benefit claim evaluation and payment, public health monitoring, research, and health care education and training. To respond to widespread consumer use of the Internet for health-related reasons, health care organizations and services

1. Cyber Dialogue, *Cyber Dialogue Releases Cybercitizen Health 2000* (Aug. 22, 2000), *at* http://www.cyberdialogue.com/news/releases/2000/08-22-cch-launch.html.

2. *Drugstores on the Net: The Benefits and Risks of Online Pharmacies, Hearings Before the Subcomm. on Oversight and Investigations of the House Comm. on Commerce*, 106th Cong. 95-96 (1999) [hereinafter *Hearings*] (statement of Janet Woodcock, Director, Center for Drug Evaluation and Research, Food and Drug Administration).

3. *Cf*. Douglas Gantenbein & Marcia Stepanek, Kaiser Takes the Cyber Cure, BUS. WK., Feb. 7, 2000, at EB 80.

must migrate from their traditional "bricks-and-mortar"[4] establishments to the Internet.[5] Until two years ago, even Kaiser Permanente, the country's largest health-maintenance organization ("HMO"), kept paper files for its patients' and shipped records around the country by traditional truck delivery.[6] Today, Kaiser and many other HMOs and health care professionals use the Internet to facilitate anything from individual account access, communication between the patient and health care provider, storage and transmission of patient data, to advice and discussion among health professionals, drug and disease research, and product ordering.[7] Before Internet health services overtake their bricks-and-mortar counterparts, the law must ensure an adequate level of confidentiality and control over consumers' personal health information; reliability of online information; and direct redress for invasions of privacy and unfair, deceptive, and fraudulent trade practices.

While online health care delivery raises many important issues, this Comment offers a comparison of the American and Canadian legal approaches to informational health privacy and Internet pharmacy sales. The United States and Canada have taken different approaches to the general protection of privacy, and this difference remains consistent between the two nations' treatment of Internet medical privacy. While the United States offers a patchwork of industry-specific privacy laws and encourages industry self-regulation, Canada has recently enacted a comprehensive privacy protection law that covers actions of both public and private actors and gives consumers a private right of action. Nonetheless, the United States has recently enacted a detailed medical privacy law. While this industry-specific law covers actions of both public and private actors, it does not give consumers a private right of action. This U.S. law is likely more comprehensive in terms of medical privacy protections because of its pinpoint focus, but it does not offer an industry-neutral, umbrella privacy protection and individual redress that the Canadian law promises. The advent of the Internet pharmacy, however, has caught both countries off guard; thus, there likely will be more consistency

4. "Bricks-and-mortar" is a term traditionally used to describe a physical facility, as opposed to a virtual establishment. "Click-and-mortar" is described as "[a] business that combines traditional retail . . . and on-line e-commerce shopping." NEWTON, *infra* note 8, at 193.

5. The number of individuals going online to retrieve health information "is growing nearly twice as fast as the Internet population at large." SCOTT REGENTS, IMPACTS OF THE INTERNET ON THE DOCTOR-PATIENT RELATIONSHIP: THE RISE OF THE INTERNET HEALTH CONSUMER 1 (1999), *available at* http://www.cyberdialogue.com/pdfs/wp/wp-cch-1999-doctors.pdf (last visited Jan. 24, 2001).

6. Gantenbein & Stepanek, *supra* note 3.

7. *See id*.

and cross-country cooperation in the future regulations of Internet pharmacy sales.

The Internet poses enhanced and unique concerns relative to informational health privacy and pharmacy sales. As technology advances and the Internet changes the way people obtain their medical services and products, protecting health information and consumers in online pharmaceutical transactions is paramount. Part II of this Comment explores the existing legal frameworks in the United States and Canada relative to informational health privacy and provides a comparative analysis of these frameworks. Part III then examines, analyzes, and compares the existing legal frameworks with regard to Internet pharmacy sales. This Comment concludes in Part IV that while the highly sensitive nature of personal medical information calls for a uniquely tailored law, a baseline umbrella privacy standard should be adopted at the federal level to provide consumers with meaningful protection and redress for all personally identifiable information. To embrace the benefits of pharmaceutical transactions via Internet and allow the medium to flourish, there should be national standards for licensure, as well as continued strict enforcement for rogue Web site operators.

II. ENHANCED AND UNIQUE CONCERNS ARISING FROM THE INTERNET

Consumer health care delivery via the Internet has moved from an embryonic idea to a pubescent reality. For purposes of this Comment, health care delivery means advice and discussion between a patient and a health care provider, access to patient and account data, and research on drugs and diseases. Consumers should be aware that this new medium for health care delivery presents unique and often hidden harms.

From a privacy protection standpoint, the architectural structure of the Internet itself presents concerns because it is a global "network of computer networks,"[8] and digital information often passes through dozens of computers before reaching its intended destination. Thus, an individual's health care information shared over the Internet is potentially more vulnerable to unauthorized access, distribution, disclosure, and general misuse than if this information had simply remained in paper form in one location. The ease with which information is created and shared over the Internet makes this grave threat of invasion of medical privacy a very real and constant concern in today's electronic age. When all records were

8. HARRY NEWTON, NEWTON'S TELECOM DICTIONARY 463 (16th ed. 2000). (A network of networks essentially means that networks of all kinds—e.g. office and home networks—around the world converge into a unified whole, the Internet.) *Id.*

maintained in paper form only and kept in the locked filing cabinet of a single physician, it was much harder to share these records with third parties and easier to guard against unauthorized access.

The advent of "cookie" technology,[9] "Web bugs," and other tracking software presents additional concerns unique to the Internet.[10] It is not far-fetched to imagine an environment where one's health insurance provider, employer, or educational institution monitors the Web sites that one visits. This would enable the insurance provider either directly or via employer tracking to have knowledge about "risky" sites an individual visits, such as HIV-positive support sites, cancer support sites, alcoholism support sites, Internet gambling sites, or pornography sites. With this knowledge, the provider may cancel coverage or simply place the individual in a higher risk category of medical coverage. Even without any overt action, the mere possession of this information by a third party, without disclosure or consent, constitutes an invasion of privacy.

Internet pharmacies present a potential for abuse that is not present, or nearly as prevalent, in traditional "bricks-and-mortar" pharmacies. The majority of medical experts agree that the Internet today offers a hodgepodge of useless and misleading information mixed in with very relevant and reliable medical information.[11] It is fair to characterize some health information on the Internet as being delivered by the snake-oil salespeople of the electronic age.[12] For example, an Internet pharmacy may heavily advertise a particular drug without disclosing that it is receiving a commission from the drug's manufacturer for every online sale of that drug. In addition, the Internet pharmacy may have chat rooms on its sites where company representatives tout the advantages of the drug, without disclosing their relationship to the Web site or the manufacturer. This mix of content and commercial purpose presents a great danger to the

9. "A 'cookie' is a small piece of information sent by a web server to store on a web browser so it can later be read back from that browser." Cookie Central, *Cookies*, *at* http://www.cookiecentral.com/cm002.htm (last visited Jan. 24, 2001). Cookies are useful for having the browser remember specific information, such as passwords, user IDs, e-mail addresses, etc. *Id.* Cookies also enable Web site tracking. *Id.*

10. "Web bugs" are tiny graphic image files embedded in a Web page, generally the same color as the background on which they are displayed, which are invisible to the naked eye and track Internet use and system capability. *See* Elizabeth Weise, *A New Wrinkle in Surfing the Net*, USA TODAY, June 7, 2000, *available at* http://www.usatoday.com/life/cyber/tech/cth582.htm.

11. *See* Catherine Calacanis, *Healthcare Goes Online*, SILICON ALLEY REP., Feb. 2000, at 106, 108.

12. Reuters, *Medical Experts Publish Guide to Web Medical Sites* (May 11, 1999), *at* http://cnn.com/HEALTH/9905/11/health.internet/index.html.

unsuspecting consumer.[13]

It might also be considerably easier to obtain prescription drugs in an online world than in an offline environment. Consumers and Web site operators might join together in this illegal activity. For example, authorities recently discovered that a Web site was selling narcotics to consumers without prescriptions or the accompanying "prescription hassles."[14] Such a scheme likely appeals to those who would like to obtain strong painkillers without going through a valid prescription process. Moreover, a rogue Internet pharmacy site may sell drugs that are not authorized in the United States or that are counterfeit reproductions of legally approved drugs. Consumers must be enabled to avoid known and unknown risks and unfair business practices in their searches for prescription drugs and other health care services on the Internet. Providing responsible and dependable health care over the Internet requires protecting personal health information, guarding against unauthorized surveillance of Web site activity, empowering consumers to find reliable and credible information and drugs via Internet pharmacies, and establishing national licensure standards for Internet pharmacies.

A. Health Privacy

Health care information is generally considered to be among the most intimate and sensitive of personal information. Even with this sensitivity, health-oriented Web sites have access to an unprecedented amount of personal information about individual consumers. For example, health-related Web sites potentially have access to information on an individual's personal and financial situation; physical health; family relationships; sexual behavior; substance abuse; and private thoughts, feelings and attitudes. Confidentiality of personal health information allows individuals to control their most intimate details and protect against the consequences of unauthorized disclosure, such as embarrassment, job loss, or societal rejection. Thus, the delivery of health care services and information via the Internet has heightened consumer fears that the confidentiality of their personal health information will be compromised. As mentioned above, health privacy concerns are only exacerbated by the Internet because of the constant threat of third-party access to patient information and the

13. Calacanis, *supra* note 11, at 108. Consumers may not understand that certain Web sites offering health-related advice or information are financially backed by companies wanting to sell their health-related products and services. Thus, consumers may not know of potential conflicts of interest. *Id.*

14. Joanna Glasner, *Narcotics: Just a Click Away?*, WIRED NEWS (Feb. 1, 2000), *at* http://www.wired. com/news/business/0,1367,41556,00.html.

proliferation of surveillance technologies, such as Web bugs and cookies.

Two recent missteps highlight the problem. First, drug companies were recently found to be paying a third-party firm, Pharmatrak, to monitor the information consumers reviewed on the drug makers' Web sites.[15] Pharmatrak's services included, among other things, reporting to the drug companies which computers downloaded information about HIV or a particular prescription drug.[16] While not directly identifying users requesting this information, the company eventually plans to match the information to user identities.[17] Second, Kaiser Permanente recently confirmed that an e-mail glitch resulted in the unintended disclosure of personal information.[18] Although quickly remedied, these instances provide further evidence of the frailties of the security measures taken to protect personal health information shared via the Internet.

Consequently, although health-related Web sites potentially provide many societal benefits, they "have not matured enough to . . . guarantee the privacy of individuals' information."[19] To continue the growth and value of online health care, an individual's personal health information must be sufficiently protected from unauthorized access and disclosure, and treated in a manner that conforms to a consumer's legitimate expectations of privacy.

Simply creating and posting privacy policies is not enough. Even when Web sites purport to offer strong privacy protections, they may ignore their own policies. The California HealthCare Foundation sponsored a study released on February 1, 2000, showing that many online health care sites do not follow their own privacy policies, and, in some cases, share health information about visitors with third-party business partners.[20] Facilitating an environment where consumers can have confidence that their intimate and sensitive personal health information will be protected and not disclosed unless authorized is necessary to the future viability of health care delivery via the Internet.

15. Robert O'Harrow, Jr., *Drug Companies Pay Firm to Track Consumers on Web*, L.A.TIMES, Aug. 17, 2000, at C1.

16. *Id.*

17. *Id*. ("'In the future, we may develop products and services which collect data that, when used in conjunction with the tracking database, could enable a direct identification of certain individual visitors.'")

18. Meghan Holohan, *Kaiser E-mail Glitch Releases Patients' Private Information*, COMPUTERWORLD (Aug. 10, 2000), *available at* http://www.computerworld.com/cwi/story/0,1199,NAV47_STO48407,00.html.

19. JANLORI GOLDMAN ET AL., CALIFORNIA HEALTHCARE FOUND., PRIVACY: REPORT ON THE PRIVACY POLICIES AND PRACTICES OF HEALTH WEB SITES 3 (2000), *available at* http://admin.chcf.org/documents/ehealth/privacywebreport.pdf (last visited Jan. 24, 2001).

20. *Id*. at 4.

B. Internet Pharmacy Sales

The sale of prescription drugs over the Internet has the potential to offer many societal benefits. For example, Internet sales of prescription drugs can foster price competition and facilitate access for the elderly and those in rural areas.[21] Internet pharmacies may generally be divided into three groups: those that merely provide a limited number of select drugs; those that are created from existing bricks-and-mortar pharmacies; and those that offer full service virtual pharmacies (e.g., drugstore.com).[22] Many pharmaceutical companies also have Web sites that provide consumer and professional information.[23] Advertisements on television, radio, and in print often direct consumers to manufacturer Web sites, which offer additional avenues for prescription drug promotion. Thus, the Internet offers a new means for consumers to gain knowledge about medical products and services and efficiently and economically obtain these products and services.

As in the medical privacy arena, online prescription drug sales present great potential for abuse. Such abuse can occur at both the vendor and consumer levels. For example, online vendors may sell counterfeit drugs, or fail to require prescriptions before distributing drugs, or consumers may supply counterfeit prescriptions to online vendors. To counter these risks, the health care industry must carefully guard against abuse and unauthorized use of various drugs, and consumers must be ensured complete, truthful disclosure about prescription medications.

The Internet provides an opportunity to circumvent strict procedural safeguards set in place to protect against both vendor and consumer abuse. Anonymity in transactions poses great risks to consumers. For example, Web-savvy entrepreneurs could establish Web sites and begin selling counterfeit drugs. Eventually, such illegal activity could be stopped; no one knows just how long it would take to discontinue the commerce, however, or how many consumers would be affected by such rogue Web site activity. Conversely, without concrete security measures, consumers could theoretically provide a single prescription to several online pharmacies to obtain additional medication, or no prescription at all to willing Web sites.

Another unique concern in the online medium is the mixture of

21. *Hearings*, *supra* note 2, at 87 (testimony of Ivan Fong, Deputy Assoc. Att'y Gen., Dep't of Justice).

22. Canadian Pharmacists Ass'n, *Statement on Internet Pharmacy in Canada* (Feb. 2000), *at* http://www.cdnpharm.ca/cphanew/HotStuff/hsframe12.htm (last visited Feb. 2, 2001) [hereinafter Canadian Pharmacists Ass'n].

23. Examples of such company Web sites include Merck (www.merck.com), Pfizer (www.pfizer.com), and Lilly (www.lilly.com).

medical content with advertising in a manner that suggests that the advertising is actually medical advice from a health care practitioner.[24] In the offline world, there are usually clear distinctions between a pharmacy and pharmaceutical manufacturer.[25] In the online world, however, a medical practitioner employed by a Web site may tout a particular drug simply because the drug's manufacturer pays for the promotion. This information is unknown to the Web site visitor and could lead to consumer deception.

III. EXISTING LEGAL FRAMEWORKS

Health care Web site owners and operators should not be able to escape the imposition of existing laws that apply to traditional bricks-and-mortar health care establishments. Recognizing the general applicability of existing laws to Internet health services is a necessary first step in defining and determining the scope and character of protections afforded to Internet health consumers and the requirements of Internet health care delivery services.

A. Informational Health Privacy

In the United States and Canada, informational health privacy is regulated at both the federal and state/province/territory levels.

1. United States

The United States has a federal system of government. Each of the fifty states has its own governmental system complemented by a national governmental framework covering the entire nation. In the context of health care services over the Internet, therefore, any such enterprise must comply with both national and state laws.

The primary enforcement mechanism for federal laws in the United States is the Department of Justice ("DOJ"). The DOJ's mission includes "enforc[ing] the law and defend[ing] the interests of the United States."[26] In addition, the Federal Trade Commission ("FTC" or "Commission") enforces a variety of consumer protection laws as well as a number of competition-promoting laws. The FTC's consumer protection mission involves eliminating deceptive or unfair acts from the marketplace.[27] Under

24. *See* Calacanis, *supra* note 11, at 108.

25. Nicholas P. Terry, *Cyber-Malpractice: Legal Exposure for Cybermedicine*, 25 AM. J.L. & MED. 327, 329 (1999).

26. DOJ, ANNUAL ACCOUNTABILITY REPORT: FISCAL YEAR 1999, at v. (2000), *available at* http://www.usdoj.gov/ag/annualreports/ar99/index.html (last visited Jan. 24, 2001).

27. FTC, *Vision, Mission & Goals*, *at* http://www.ftc.gov/ftc/mission.htm (last

the Federal Trade Commission Act ("FTC Act"), the FTC is empowered to prevent unfair methods of competition and "unfair or deceptive acts or practices in or affecting commerce,"[28] prescribe trade regulation rules defining acts that are unfair or deceptive, and establish requirements designed to prevent such acts or practices.[29] As a result, one of the Commission's major policy initiatives since 1995 has been to address online privacy.[30]

The Internet has experienced widespread growth since 1990. From 1990 to 1997, the "estimated number of Internet users grew from around one million to around 70 million."[31] Thus, the Clinton Administration was the first to play a key role in formulating Internet policy. To facilitate the growth of the Internet and electronic commerce, the Clinton Administration developed a general policy that "includes support for industry self-regulation where possible, technology-neutral laws and regulations, and an appreciation of the Internet as an important medium . . . for commerce."[32] This policy has helped to facilitate the dramatic and widespread adoption of the Internet as a valuable communications, information, and electronic commerce medium.

a. Federal law

The Internet has fueled interstate commerce, which in turn has produced a growing body of laws with provisions covering the confidentiality of medical records and information. Most federal laws merely address the handling of personally identifiable health information by federal agencies and their private subcontractors. For example, the Privacy Act of 1974 provides a system of confidentiality protections that

modified June 17, 1999).

28. 15 U.S.C. § 45(a)(1) (1994).

29. *Id.* §§ 41-58.

30. In the fall of 1995, the FTC held extensive hearings on the implications of globalization and technological innovation for both competition and consumer protection. The hearings were summarized in a staff report entitled ANTICIPATING THE 21ST CENTURY: CONSUMER PROTECTION POLICY IN THE NEW HIGH-TECH, GLOBAL MARKETPLACE (1996), *available at* http://www.ftc.gov/opp/global/report/gc_v1.pdf (last visited Jan. 24, 2001). Since that time, the Commission has produced four reports on the subject of online information collection practices. The FTC released the latest report in May 2000. FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE A REPORT TO CONGRESS (May 2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (last visited Jan. 24, 2001) [hereinafter PRIVACY ONLINE]

31. THE MANAGEMENT OF INTERNET NAMES AND ADDRESSES: INTELLECTUAL PROPERTY ISSUES: FINAL REPORT OF THE WIPO INTERNET DOMAIN NAME PROCESS para. 2(i) (1999), *available at* http://wipo2.wipo.int/process1/report/pdf/report.pdf (last visited Jan. 24, 2001).

32. *Hearings*, *supra* note 2, at 87 (testimony of Ivan Fong).

apply to individual records, including medical histories,[33] when that information is retained by federal agencies.[34] Other federal statutes have been used to address at least some medical records issues. These include the Health and Human Services ("HHS")-sponsored statute to require Medicare + Choice organizations to establish safeguards for maintaining the privacy of health information;[35] the Inspector General Act of 1978, which authorizes the Inspector General's office to access records, documents, and other materials for its purposes;[36] the Americans with Disabilities Act;[37] the Controlled Substances Act;[38] and the Comprehensive Alcohol Abuse & Alcoholism Prevention, Treatment & Rehabilitation Act of 1970.[39]

1. Department of Health and Human Services

In August of 1996, former President Clinton and Congress took an important step toward regulating the conduct of private actors by enacting the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[40] One of the primary purposes of HIPAA was to facilitate the electronic storage and distribution of health information.[41] In addition, HIPAA was intended to address the "need for national standards to control the flow of sensitive patient information and to establish real penalties for the misuse or disclosure of this information."[42] Toward this end, HIPAA gave HHS the authority to promulgate binding regulations on the use of personally identifiable health information in certain transactions if Congress failed to enact medical confidentiality legislation by August 21, 1999.[43] After this deadline passed without any such federal legislation, HHS issued a proposed Health Information Privacy Rule on November 3,

33. 5 U.S.C. § 552a(a)(4) (1994).

34. Privacy Act of 1974, Pub. L. No. 93-573, § 2(b), 88 Stat. 1896, 1897.

35. Balanced Budget Act of 1997 § 4001, 42 U.S.C. § 1395w-22(h) (Supp. IV 1998).

36. Inspector General Act of 1978, 5 U.S.C. app. § 6 (1994).

37. 42 U.S.C. § 12112(d)(3)(B).

38. 21 U.S.C. § 872(c).

39. 42 U.S.C. § 290dd-2, *amended by* 42 U.S.C. § 290dd-2(e) (Supp. IV 1998).

40. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936 (codified at scattered sections of 26, 29, and 42 U.S.C.).

41. DEP'T OF HEALTH AND HUMAN SERVS., IMPLEMENTATION OF ADMINISTRATIVE SIMPLIFICATION REQUIREMENTS BY HHS, *at* http://aspe.os.dhhs.gov/admnsimp/kkimpl.htm (last updated Aug. 24, 1998).

42. DEP'T OF HEALTH AND HUMAN SERVS., HHS FACT SHEET: PROTECTING THE PRIVACY OF PATIENTS' MEDICAL RECORDS (2000), *available at* http://www.hhs.gov/news/press/2000pres/00fsprivacy.html (last visited Feb. 5, 2001) [hereinafter HHS FACT SHEET].

43. *Id*.

1999.[44] On December 20, 2000, the HHS Secretary announced the final regulations ("Privacy Rule"), which became effective on February 26, 2001.[45]

In the view of the HHS Secretary, the key principles necessary in a federal privacy law were consumer control, accountability, public responsibility, boundaries, and security.[46] In fulfilling these principles, the Privacy Rule establishes a set of basic national privacy standards and fair information practices that protect Americans' personally identifiable health information.[47] Specifically, it: (1) ensures patient access to their medical records; (2) requires patient consent before individually identifiable health information is used and shared for purposes of treatment and payment; (3) establishes fair information practices to inform patients how their personal information is used and disclosed; (4) requires safeguards to protect confidentiality and prevent unauthorized access; and (5) establishes penalties for misuse of personal health information.[48]

In giving patients greater access to and control over their personal health information and providing boundaries for use and security of that information, the Privacy Rule directly applies only to health plans, health care clearinghouses, and health care providers who transmit health information in electronic form ("covered entities") in their use and disclosure of "protected health information."[49] "Protected health information" is defined as "individually identifiable health information" regardless of its form or format.[50] In certain situations, the Privacy Rule also applies to a covered entity's business associates. While business associates retained by covered entities (lawyers, accountants, consultants, etc.) to perform certain services are not directly covered by the Privacy Rule, covered entities must contractually require the protection of protected health information when business associates have the right to use or disclose the protected health information belonging to the covered entity.[51]

44. *See* 64 Fed. Reg. 59,917 (Nov. 3, 1999).

45. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160, 164).

46. "Boundaries" indicate that generally an individual's health care information is to be used for health purposes only. HHS FACT SHEET, *supra* note 42.

47. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,463-74.

48. HHS FACT SHEET, *supra* note 42.

49. Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. § 160.102(a). Under HIPAA section 1171(a), only these three entities could be covered under a final privacy rule. The Health Insurance Portability and Accountability Act of 1996 § 1171(a), 42 U.S.C. § 1320d (Supp. IV 1998).

50. 45 C.F.R. § 164.501 (2001).

51. *Id*. §§ 160.103, 164.502(e)(2).

The Privacy Rule places meaningful limits on the flow of protected information. For instance, a covered entity must make all reasonable efforts not to use or disclose more than the minimum amount of protected information necessary to accomplish the intended purpose.[52] When use or disclosure of protected health information is necessary, a covered entity must generally obtain the individual's consent before using this information to carry out treatment, payment, or health care operations.[53] Additionally, covered entities are encouraged to use "de-identified" information, stripped of elements that could be used to identify individuals.[54] Once information has been "de-identified," it may be used or disclosed without restriction.[55] Finally, the Privacy Rule restricts employer access to information for purposes other than health care.[56]

While the Privacy Rule represents the first comprehensive federal law that protects the confidentiality of personally identifiable health information, it has some gaps in its protection. First, there is no private right of individual action for inappropriate use of medical data.[57] A private right of action is important because it gives consumers direct redress for harms to their personal privacy. In addition, a private right of action encourages consumers to be more vigilant guardians of their sensitive medical information, whereas the Privacy Rule encourages more unauthorized activity with less public monitoring and safeguarding. Second, HHS does not have authority to issue standards for records maintained by other insurers, employers, or schools because the "covered entities" section limits the specific entities governed by the requirements.[58] Third, the Privacy Rule does not directly place restrictions on the use or disclosure of information by business associates.[59] Fourth, covered entities

52. *Id.* § 164.502(b)(1).

53. *Id.* § 164.506(a).

54. *Id.* § 164.502(d).

55. *Id*.

56. *Id.* § 164.512(b)(1)(v).

57. This defect results from the fact that Congress did not authorize such an enforcement mechanism. Nonetheless, HIPAA does provide for civil penalties for a failure to comply with the requirements and standards, and criminal penalties for certain wrongful disclosures. The Health Insurance Portability and Accountability Act of 1996 §§ 1176, 1177, 42 U.S.C. 1320d-5 (Supp. IV 1998).

58. 45 C.F.R. § 160.102. Again, this defect is a result of HIPAA's statutory limits.

59. This fourth element is noteworthy because of the recent public outcry concerning DoubleClick's (a third party business partner to many health care Web sites) use of targeted promotional messages. Recently, a California woman filed a lawsuit against the company alleging violation of privacy rights and deceptive practices. Allegedly, she received a barrage of unsolicited e-mails from insurers, loan companies, and others after she looked up medical insurance information online. Heather Green et al., *Privacy: Outrage on the Web*, BUS. WK., Feb. 14, 2000, at 38. If business partners and all holders of personally

are permitted to disclose protected health information to law enforcement officials pursuant to administrative subpoenas or summons without independent judicial review.[60]

Perhaps most relevant to this Comment, the majority of health care Web sites may not meet the statutory definition of "covered entities" under the proposed Privacy Rule, and will therefore not be subject to its requirements.[61] Nonetheless, it is likely that many health care Web sites have business plans to eventually offer or support services that make them "business associates" of health plans or health care providers for the purposes of the regulation. To the extent that this occurs, it will be imperative that health care Web sites demonstrate to their covered entity business associates that their privacy policies, data handling practices and procedures, business arrangements with third parties, personnel management, and technical security arrangements meet or exceed the standards of the Privacy Rule.[62]

2. Federal Trade Commission

In addition to the above detailed medical privacy law, the FTC is responsible for enforcing the nation's consumer protection laws, which protect consumers from deceptive trade practices.[63]

As mentioned above, the FTC has focused considerable attention and resources on issues related to the collection and dissemination of personal information on the Internet. In its 2000 report, *Privacy Online: Fair Information Practices in the Electronic Marketplace*, the FTC stated that the "failure to comply with stated information practices may constitute a

identifiable information are not directly restricted in use and disclosure by the Privacy Rule, more assaults on sensitive medical information will occur.

60. 45 C.F.R § 164.512(f)(1)(ii)(C). Other warrants and nongrand jury subpoenas or summons require independent judicial review. *Id.* § 164.512(f)(1)(ii)(A).

61. *Id.* § 160.102. The closest definition to a health care Web site is a health care provider. The Privacy Rule defines "health care provider" as the Social Security Act does in 42 U.S.C §§ 1395x(u): a provider of services, meaning a "hospital, critical access hospital, skilled nursing facility, comprehensive outpatient rehabilitation facility, home health agency, hospice program;" and in § 1395x(s) as a provider or medical or health services, such as physician, hospital and diagnostic services; and also as "any person or organization who furnishes, bills, or is paid for health care services in the normal course of business." 45 C.F.R § 160.103. This definition likely includes researchers who provide health care to research subjects, free clinics, and health clinics or licensed health care professionals located at schools or business.

62. This includes providing "satisfactory assurances that the business associate will appropriately safeguard information. 45 C.F.R. § 164.502(e)(1)(i).

63. *See* 15 U.S.C. §§ 41-58 (1994). Specifically relevant in the privacy context, section 5(a) of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce." *Id.* § 45(a).

deceptive practice . . . and the Commission has authority to pursue the remedies available under the Act for such violations."[64]

The FTC has used its authority under section 5 of the FTC Act to prosecute companies whose practices do not live up to the privacy policies posted on their Web sites.[65] Health care Web sites can be prosecuted under section 5 of the FTC Act for violations of their privacy policies because the FTC does not treat health care Web sites differently than any other Web sites. In addition to enforcing privacy policies, the FTC has examined the role of self-regulation, technology-based privacy solutions, and the special case of children's privacy.[66] The Commission has recently endorsed a self-regulatory framework developed by the Network Advertising Initiative,[67] while at the same time calling for baseline privacy legislation.[68] While continuing to encourage online privacy through self-regulation, the FTC believes that a stopgap legislative measure is necessary to fully ensure that consumer privacy is protected online.[69]

The legislation envisioned by the Commission in its report to Congress on online profiling would "set forth a basic level of privacy protection for all visitors to consumer-oriented commercial Web sites with

64. PRIVACY ONLINE, *supra* note 30, at 34.

65. The FTC has brought cases against several companies that failed to follow their own privacy policies. *See id.* at 42 (stating that FTC has brought cases against GeoCities, Liberty Financial and ReverseAuction); FTC, *FTC Sues Failed Website, Toysmart.com for Deceptively Offering for Sale Personal Information of Website Visitors* (July 10, 2000), *at* http://www.ftc.gov/opa/2000/07/toysmart.htm; FTC, *Online Pharmacies Settle FTC Charges* (July 12, 2000), *at* http://www.ftc.gov/opa/2000/07/iog.htm.

66. PRIVACY ONLINE, *supra* note 30, at 42 n.21. Based on survey research showing that Web sites that target children often collected information, the FTC concluded that legislation was necessary to protect the online privacy of children. *Id*. at 4. Congress responded by passing the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. §§ 6501-6506 (Supp. IV 1998).

67. Formally announced at the Department of Commerce/FTC Public Workshop on Online Profiling, held November 8, 1999, Network Advertising Initiative is an organization comprised of leading Internet advertisers. Network Advertising Initiative, *Testimony at the Online Profiling Workshop*, *at* http://www.networkadvertising.org/press/11-9-99testimony.shtml (last visited Jan. 27, 2001).

68. FTC, ONLINE PROFILING: A REPORT TO CONGRESS PART 2 RECOMMENDATIONS 4 (2000), *available at* http://www.ftc.gov/os/2000/07/onlineprofiling.pdf (last visited Jan. 27, 2001).

69. *See id.* at 9-10. Commissioner Orson Swindle disagreed that legislation was needed as a backstop and therefore dissented from this recommendation. He characterized legislation mandating the four fair information practices (notice, choice, access, and security) as overly burdensome and unwarranted. *Id.* cmt. (Dissenting Statement of Comm'r Swindle). Commissioner Thomas Leary agreed that some legislation was needed but suggested that legislation focus on adequate notice and not across-the-board standards for fair information practices. *Id.* cmt. (Statement of Comm'r Leary Concurring in Part and Dissenting in Part).

respect to profiling."[70] The FTC suggests that such legislation provide an implementing agency with the authority to: (1) promulgate more detailed standards; (2) enforce those standards; and (3) grant safe harbors to self-regulatory principles that effectively implement the standards of fair information practices detailed in the legislation and subsequent rulemaking.[71]

b. State law

Individual states currently provide a patchwork of laws and regulations addressing health care information and records. In the most comprehensive study of state health privacy laws to date, the Georgetown Health Privacy Project noted that "[s]tate laws relating to health privacy have been enacted at different points in time, over many years, and address a wide variety of uses and public health concerns."[72] Nonetheless, providing health services over the Internet is a multi-jurisdictional activity that could, in theory, implicate the laws of all fifty states.

Moreover, HHS's Privacy Rule under HIPAA does not necessarily preempt state law.[73] Instead, the federal standards under HIPAA are intended to enhance the privacy protections offered in existing state laws.[74] Where state and federal laws relating to the privacy of personally identifiable information conflict, the stronger privacy protection will prevail.[75] Lastly, individual states are also free to enact more stringent standards and requirements with respect to disclosure or the rights of individuals to access or amend their individually identifiable information.[76]

70. *Id.* at 10.

71. *Id*.

72. HEALTH PRIVACY PROJECT, GEORGETOWN UNIVERSITY INSTITUTE FOR HEALTH CARE RESEARCH AND POLICY, THE STATE OF HEALTH PRIVACY: AN UNEVEN TERRAIN, Executive Summary (1999), *at* http://www.healthprivacy.org/usr_doc/33779.pdf (last visited Feb. 1, 2001).

73. Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. § 160.201 (2001). This limitation is due to the language in section 1178 of HIPAA. Health Insurance Portability and Accountability Act of 1996 § 1178, 42 U.S.C. § 1320d-7 (Supp. IV 1998).

74. As a general rule, state laws that are contrary to standards or implementation specifications, such as those under the Privacy Rule, are preempted. 42 U.S.C. § 1320d-7. The statute provides an exception to this preemption for state laws that are more stringent than the federal requirements. *Id.*

75. Health Insurance Portability and Accountability Act of 1996 § 264(c)(2), 110 Stat. at 2033; *see also* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,922 (Nov. 3, 1999) (explaining that section 264's preemption provision provides that "contrary provisions of State laws that are more stringent than the federal standards, requirements, or implementation specifications will not be preempted").

76. 45 C.F.R. §§ 160.202, 160.203(b).

This is because the Privacy Rule is intended to establish a floor, not a ceiling, on privacy protections.[77]

A seminal case on the ability of states to collect personally identifiable information as it relates to use of prescription drugs of a certain caliber (e.g., drugs having a potential for abuse and also a recognized medical use) is the Supreme Court case of *Whalen v. Roe*.[78] The New York statute at issue required physicians to provide the New York State Department of Health in Albany with prescription information, which was then recorded in a centralized computer file.[79] In *Whalen*, the Court reversed a decision by the District Court for the Southern District of New York, and held that: (1) the personally identifiable requirement was a reasonable exercise of the state's broad police powers;[80] (2) the statute, on its face, was not an invasion of the right to privacy or any other right or liberty protected by the Fourteenth Amendment;[81] and (3) the statute did not impair the physician's right to practice medicine free of state interference.[82]

In denying the privacy interest, the Court reasoned that the security provisions in New York's statute prohibiting public disclosure of the personally identifiable information would be properly administered.[83] In addition, the Court reasoned that disclosure of the private information to authorized employees did not automatically amount to an impermissible invasion of privacy.[84] The Court was careful to limit its holding to the record before it, however, and noted that this record by itself did not constitute an invasion of the liberties protected by the Fourteenth Amendment.[85] Thus, a different set of facts, such as when protection of an individual's interest in privacy is not adequately guarded, might cause enough concern for the Court to overrule a similar state statute. The *Whalen* case is important because it shows that although many state laws carry good privacy protections, states have broad authority to enact laws that infringe on medical privacy interests under the constitutional guise of their police powers.

77. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,463-74 (Dec. 28, 2000).

78. 429 U.S. 589 (1977).

79. *Id*. at 593.

80. *Id*. at 598.

81. *Id*. at 600.

82. *Id*. at 604.

83. *Id*. at 601.

84. *Id*. at 602.

85. *Id*. at 605-06.

2. Canada

In contrast to the United States, Canada has a parliamentary system of government. In each of Canada's ten provinces, there is a legislature, and for every province except Ontario, there is an appointed Upper House—the Legislative Council—and an elected Lower House—the Legislative Assembly. Like the United States, Canada operates under a federalist system. This includes a strong central government and Parliament, combined with an ample measure of autonomy and self-government for each of the federated communities.[86]

Canada's constitution, unlike that of the United States, incorporates many documents.[87] The Constitution Act of 1982 sets out the Canadian Charter of Rights and Freedoms.[88] The rights guaranteed by the Charter are: (1) fundamental freedoms (conscience, religion, thought, belief, opinion and expression, peaceful assembly, and association); (2) democratic rights; (3) mobility rights; (4) legal rights; (5) equality rights; (6) official language rights; and (7) minority language education rights in certain circumstances.[89] All these rights are "subject only to such reasonable limits . . . as can be demonstrably justified in a free and democratic society."[90]

a. Federal law

Like the United States, Canadian federal privacy law addresses the handling of personal health information by federal agencies and their private subcontractors. The Canadian Privacy Act ("Privacy Act") gives Canadian citizens and people present in Canada the right to have access to information about them held by any listed "department or ministry of state of the government of Canada."[91] Because Canada offers a single-payer system of health care,[92] some government operations use personal

86. Canada's ten provinces are Alberta, British Columbia, Prince Edward Island, Manitoba, New Brunswick, Nova Scotia, Ontario, Québec, Saskatchewan, and Newfoundland and Labrador. Canada's three territories include the Northwest Territories, Nunavut, and the Yukon Territory. Government of Canada, *Canada*, *at* http://canada.gc.ca/canadiana/lmap_e.html (last visited Jan. 27, 2001).

87. Canadian Embassy, *Canada's Constitution*, *available at* http://www.canadianembassy.org/issues/federalism/constitution.html (last visited Jan. 27, 2001).

88. CAN. CONST. (Constitution Act, 1982) pt. I (Canadian Charter of Rights and Freedoms), §§ 2-23.

89. *Id*.

90. *Id*. § 1.

91. Privacy Act, R.S.C., ch. P-21, §§ 2-3 (1985) (Can.).

92. This is not to be confused with a "socialized medicine" system in which doctors are employed by the government. Canada's system involves private practitioners who are generally paid on a fee-for-service basis. Canadian provinces and territories plan, finance, and evaluate hospital care, physician services, and some aspects of prescription care and

information about individuals, such as health promotion programs at Health Canada[93] and income tax programs at Revenue Canada.[94] In addition to the right of access, individuals may request that any errors be corrected and, if a request is refused, require that a notation be attached to the information describing any corrections requested but not made.[95] The Privacy Act also protects against unauthorized disclosure of personal information.[96] In addition, the Privacy Act strictly controls how the government will collect, use, store, disclose, and dispose of any personal information.[97]

The Privacy Act requires the federal government to: (1) limit its collection of personal information to the minimum details needed to operate programs or activities; (2) collect the information, whenever possible, directly from the person concerned; (3) tell the person why the information is being collected and how it will be used; (4) not use the information for other purposes, unless allowed by law; (5) keep the information long enough to allow the person a reasonable opportunity to obtain access; (6) ensure the information is as accurate, up-to-date and complete as possible; and (7) not disclose personal information unless specifically allowed by the Privacy Act or another law.[98] Since the Privacy Act took effect, Canadians have enjoyed a right to privacy with respect to their health information and federal government records.[99] While the medical records themselves belong to the physician, patients are entitled to examine and copy all of their medical records.[100]

In addition to the protections afforded by the Privacy Act, in August 1998, the Canadian Medical Association approved the Health Information Privacy Code ("CMA Code"), which offers an industry self-regulatory mechanism for protecting personal health information.[101] The CMA Code

public health. This is the single-payer system. Health Canada, *About Health Canada*, *at* http://www.hc-sc.gc.ca/english/about.htm (last visited Jan. 27, 2000).

93. *Id*. Health Canada is the federal department responsible for developing health policy, enforcing health regulations, promoting disease prevention and enhancing healthy living for all Canadians. *Id.* Health Canada ensures that health services are available and accessible to Canadian citizens. *Id.*

94. Canada Revenue and Customs Agency, *Who We Are*, *at* http://www.ccra-adrc.gc.ca/agency/menu-e.html (last visited Jan. 27, 2001). Revenue Canada is the federal department responsible for tax, trade, and border legislation and regulations. *Id.*

95. Privacy Act, R.S.C., ch. P-21, § 12(1)-(2) (1985) (Can.).

96. *Id*. § 8(1).

97. *Id*. §§ 4-6.

98. Privacy Act, R.S.C., ch. P-21, §§ 4-8(1) (1985) (Can.).

99. *Id*.

100. McInerny v. MacDonald, [1992] 2 S.C.R. 138 (establishing a common law right of access to one's own medical records).

101. Canadian Medical Ass'n, *CMA Health Information Privacy Code*, *at*

articulates principles for protecting "the privacy of . . . patients, the confidentiality and security of . . . health information and the trust and integrity of the therapeutic relationship," and "applies to all health information and to all individuals, groups or organizations that collect, use, disclose or access such information."[102] Although this CMA Code is noteworthy because it sets standards and creates awareness of the importance of confidentiality of personal medical information, it lacks effective enforcement mechanisms.[103] Because the CMA Code is a self-regulatory program, health custodians subject to it must merely subscribe to the principles and agree to uphold them; the CMA Code does not provide for further enforcement for violations or tracking.[104]

Possibly the biggest hole in Canadian privacy protections was the lack of a general privacy law applicable to private actors. The Internet and the explosion of electronic commerce have unequivocally pointed to the need for stronger privacy protections from unaccountable private actors. The Government of Canada responded to this need. In October 1998, the Personal Information Protection and Electronic Documents Act ("PIPED Act") was introduced in the House of Commons,[105] and it was enacted on April 13, 2000.[106]

The PIPED Act introduced measures to protect personal information in the private sector, created an electronic alternative for doing business with the federal government, and clarified how courts assess the reliability of electronic records used as evidence.[107] The PIPED Act will apply to *all* organizations that collect, use, or disclose personal information.[108] Thus, theoretically, this bill could apply to both domestic and foreign organizations.

Beginning January 1, 2002, with a few exceptions, any federally regulated industry organization that uses, collects, or discloses personally identifiable information in the course of commercial activity, must protect that information by complying with a set of ten principles based on the Canadian Standards Association's Model Privacy Code for the Protection

http://www.cma.ca/inside/policybase/1998/09-16.htm (last visited Jan. 27, 2001).

102. *Id*. § A.

103. *See id*.

104. *See id.*

105. Bill C-6, *Personal Information Protection and Electronic Documents Act*, 2d. Sess., 36th Parl., 1999, *available at* http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6TOCE.html.

106. Personal Information Protection and Electronic Documents Act, S.C., ch. 5 (2000) (Can.).

107. *Id*.

108. *Id*. § 3.

of Personal Information ("Model Code").[109] The law will not apply to organizations that handle personal health information for commercial purposes until January 1, 2002.[110] On January 1, 2004, the law will extend to all non-federal businesses that handle personal information for commercial purposes.[111] Organizations that handle information for journalistic, artistic, law enforcement, and specifically non-commercial purposes are exempt from the law, as are individuals who handle information solely for "personal or domestic purposes."[112]

The Model Code's ten principles, which are given legal effect by their incorporation into Schedule 1 of the PIPED Act,[113] require covered entities to ensure accountability for complying with the provisions; identify purposes for collecting personal information; obtain consent for such collection; limit the amount of data collected to only what is needed; limit the subsequent use, disclosure, and retention of the collected information; ensure the information's accuracy; institute safeguards to protect the data collected; make data collection and maintenance policies readily available; allow individuals to access their own data; and accept and address individual challenges regarding the entity's compliance with the provisions.[114] An individual who suspects that an organization is not in full compliance with the privacy protection principles and cannot settle the matter with that organization may then bring a case before Canada's Privacy Commissioner, who will seek to resolve the dispute.[115] Unresolved disputes will be taken before the Federal Court, which may order the organization to correct its practices and award damages to the complainant, including damages for "humiliation that the complainant has suffered."[116] In addition, anyone found guilty of obstructing an investigation by the Commissioner may be fined up to $100,000.[117]

Where a province or a territory adopts substantially similar legislation, the organizations covered by the provincial or territorial legislation will be exempted from the application of the federal law within

109. Industry Canada, Electronic Commerce in Canada, *Privacy: The Protection of Personal Information*, *at* http://www.ecom.ic.gc.ca/english/privacy/632d30.html (last visited Jan. 27, 2001) [hereinafter *Protection of Personal Information*].

110. *Id*.

111. *Id*.

112. Personal Information Protection and Electronic Documents Act, S.C., ch. 5, § 4 (2000) (Can.).

113. *Protection of Personal Information*, *supra* note 109.

114. Personal Information Protection and Electronic Documents Act, S.C., ch. 5, sch.1, § 4 (2000) (Can.).

115. *Id*. § 11(1).

116. *Id*. § 16(c).

117. *Id*. § 28(b).

that jurisdiction.[118] Québec already has substantially similar privacy legislation covering the private sector, so organizations collecting, using, or disclosing personal information within the province will be exempted from the application of the federal bill.[119] The federal legislation complements Québec's private sector privacy law by covering federally regulated organizations such as banks and airlines, as well as interprovincial and international data flows.[120]

b. Province and Territory law

The individual provinces in Canada have enacted their own privacy laws. Unlike laws enacted by the individual states in the United States, these laws generally cover personal information in hospitals, mental health centers, health units, and student/employee health centers located in provincial or local government offices or post-secondary institutions.[121] These medical facilities are government-provided services and thus subject to existing privacy laws applicable to government actors—not because private physician services fall subject to privacy legislation.

The Canadian province of Québec stands as an exception to this, as it has enacted privacy legislation applicable to private actors.[122] Thus, in Canada, there is not only a chasm between health privacy regulations covering government and private actors, but each province differs in the specific privacy protections afforded to its citizenry.[123] Nonetheless, much of the existing and new legislation has been criticized as empowering provincial governments to "breach patient-physician privacy by allowing

118. *Protection of Personal Information*, *supra* note 109.

119. In January 1994, Québec enacted Bill 68, which extended the right of access to personal information held by credit bureaus, insurance companies, pharmacies, and any other commercial enterprises that hold personal information. *See* An Act Respecting the Protection of Personal Information in the Private Sector, S.Q., ch. 17 (1993) (Can.).

120. Personal Information Protection and Electronic Documents Act, S.C., ch. 5, § 2(1) (2000) (Can.).

121. *See* Freedom of Information and Protection of Privacy ("FOIP") Act, S.A., ch. F-18.5 (1994) (Can.) (aiming to strike a balance between the public's right to know and the individual's right to privacy, as these rights relate to information held by the Government of Alberta). Ontario and British Columbia have also adopted Freedom of Information and Protection of Privacy Acts. *See* Freedom of Information and Privacy Act, R.S.O., ch. F.31 (1990) (Can.); Freedom of Information and Privacy Act, R.S.B.C., ch. 165 (1996) (Can.).

122. *See* An Act Respecting the Protection of Personal Information in the Private Sector, S.Q., ch. 17 (1993) (Can.).

123. *See* Miro Cernetig, *Drug Company Sues to Obtain B.C. Data*, THE GLOBE AND MAIL (Apr. 3, 1998), at A10, *available at* http://ptg.djnr.com/ccroot/asp/publib/story.asp. The British Columbia "government's decision to stop pharmacies from selling information about drug sales to the private sector [was] challenged in the B.C. Supreme Court." *Id.* Right now, British Columbia is the only province in Canada that prohibits pharmacists from providing detailed data on drug sales to companies. *Id.*

them and others to access electronic health records."[124]

In January of 1998, Industry Canada[125] issued a discussion paper entitled "The Protection of Personal Information: Building Canada's Information Economy and Society."[126] The paper requested public comment concerning the specific structure and function of proposed federal legislation to regulate the collection, use, and disclosure of personal information in the private sector.[127] In response to this request, British Columbia's Privacy Commissioner made a number of recommendations, including: (1) that the Government of Canada and the provincial legislatures introduce statutory privacy rights for the protection of personal information held by private actors; (2) that this legislation establish a statutory requirement of informed consent; and (3) that this legislation further establish enforceable legal rights to *fair information practices*.[128] Thus, like their American counterparts, many Canadian citizens have expressed a desire for a uniform statutory response to address the privacy of personally identifiable information on the Internet.

3. Analysis of Informational Health Privacy Laws in the United States and Canada

a. Similarities

Until recently, there were two primary similarities between the laws in the United States and Canada. First, both countries offered a patchwork of privacy protections that differed from state to state or province to province. Second, both countries had federal privacy laws that regulated the conduct of government actors, but not that of private actors. Today, both countries still offer a highly variable set of privacy protections

124. Gordon Atherley, *Sneaking a Peak*, 34 THE MEDICAL POST (Feb. 24, 1998), *available at* http://www.medicalpost.com/mdlink/english/members/medpost/data/3408/09.htm.

125. Industry Canada is a federal department designed to foster a competitive Canadian economy. Industry Canada is involved in a multitude of activities such as setting telecommunications policy and promoting investment and trade. *See* Industry Canada, *About Industry Canada*, *at* http://www.ic.gc.ca/cmb/Welcomeic.nsf/ICPages/AboutIndustryCanada (last visited Jan. 30, 2001).

126. INDUSTRY CANADA, PRIVACY: THE PROTECTION OF PERSONAL INFORMATION (1998), *available at* http://www.e-com.ic.gc.ca/english/privacy/632d2.html (last visited Jan. 27, 2001).

127. *Id*. pt. 3.

128. The Commissioner noted that these recommendations are fundamental principles of the European Union's Directive on Data Protection and should be reflected in Canadian law. David H. Flaherty, Submission to Industry Canada Re: The Information Highway (Dec. 22, 1994), *available at* http://www.oipcbc.org/publications/other/Industry-Canada.html.

depending on a person's physical geographical location within each country. Canada, however, has repaired its public/private dichotomy with the passage of the PIPED Act. With respect to personally identifiable health information, the United States has also adopted a comprehensive federal law aimed at private actors. Until the PIPED Act and the Privacy Rule came into being, the Canadian and American legal privacy frameworks were substantially similar in the privacy protections that they afforded to individuals.

b. Differences

One of the most striking differences between Canada and the United States in terms of national structure resides in their respective health care systems. While the United States has a privatized system requiring citizens to pay for their own health care programs and services (privately financed and privately delivered), Canada offers a predominantly publicly financed, privately delivered health care system. The Canadian system, known as "Medicare," "provides access to universal, comprehensive coverage for medically necessary hospital, in-patient and out-patient physician services."[129] This difference in health care structure results in differing regulation of health care providers with respect to personally identifiable patient data.

Furthermore, the United States and Canada differ in their approaches to privacy in general, and specifically with regard to informational health privacy. As an initial matter, since 1977 Canada has had a politically appointed position of federal Privacy Commissioner that is accountable to Parliament.[130] The Canadian Privacy Commissioner surely gives a citizen a certain level of comfort that reported invasions of privacy would be investigated and, where necessary, prosecuted. By contrast, the American system offers no such direct point of contact for information privacy violations against a citizen. The FTC has broad authority to investigate and prosecute unfair and deceptive trade practices when a Web site has violated its own posted privacy policy; however, this does not grant the citizenry any special protections or private rights of action.

Moreover, Canada's recent enactment of the PIPED Act provides a broad-based privacy protection initiative. Aside from laws geared at industry-specific private actors (e.g., video rental industry, cable TV

129. HEALTH SYSTEM AND POLICY DIVISION OF HEALTH CANADA, CANADA'S HEALTH CARE SYSTEM 1 (1999), *at* http://www.hc-sc.gc.ca/datapcb/datahesa/hlthsys/Ehlthsys.pdf (last visited Feb. 1, 2001).

130. Privacy Comm'r of Canada, *Our Mission and Our Mandate*, *at* http://www.privcom.gc.ca/english/02_01_e.htm (last visited Feb. 1, 2001).

industry), the United States does not have a comprehensive or umbrella privacy law in place. Such industry-specific laws include the Video Privacy Protection Act,[131] which attempted to curb privacy disclosures and privacy invasions of consumers renting videos, and the Cable Communications Policy Act[132] with similar privacy provisions.

While HHS's Privacy Rule under HIPAA constitutes a landmark step in protecting the confidentiality of personal medical information, it continues a legacy of industry-specific, patchwork privacy protection, instead of a broad-based privacy protection mechanism. In addition, as discussed earlier, the Privacy Rule in its present definition of "covered entities"[133] may not directly implicate health-related Web sites. It may reach these Web sites, however, through the restrictions laid out for defined "business associates," or through the offered definition of health care providers. Finally, the Privacy Rule does not offer a private right of action. Thus, the American consumer is somewhat left without remedy from individual invasions of privacy. By contrast, the Canadian efforts seem to support a more genuine overarching privacy protection goal for its citizenry, rather than the patchwork, sector-by-sector focus of the United States's privacy protection framework.

c. Reasoning for Similarities and Differences

To address alleged privacy violations, Canada maintains a national Privacy Commissioner, as do some provinces.[134] Thus, in relation to the United States, Canada is much more advanced on the implementation side of privacy policy because of the existence of these official positions, which are designed to balance greater openness and accountability for general information against the protection of personal information of the citizenry. When Americans encounter privacy obstacles or invasions, they usually have to sue in courts to achieve common-law redress,[135] whereas in Canada, affected citizens may first obtain the backing and prosecutorial support of

131. 18 U.S.C. § 2710 (1994).

132. 47 U.S.C. § 551 (1994).

133. HIPAA limits application of the Privacy Rule to the following "covered entities:" (1) health plans, (2) health care clearinghouses, and (3) health care providers who transmit health information in electronic form in connection with transactions referred to in section 1173(a)(1)of the Act. Health Insurance Portability and Accountability Act of 1996 § 1172, 42 U.S.C. § 1320d-1 (Supp. IV 1998).

134. *See* Privacy Comm'r of Canada, *Information and Privacy Organizations in Canada*, *at* http://www.privcom.gc.ca/ english/02_03_01_e.htm (last visited Feb. 1, 2001).

135. There are four so-called common-law "privacy torts." These include intrusion on seclusion or solitude, public disclosure of private facts, publicity in a false light, and appropriation of name or likeness. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 388-89 (1960).

the Privacy Commissioner.[136]

From a policy standpoint, the Canadian government may value privacy more than it values capitalism and freedom of enterprise, or simply view privacy as an economy-building tool. By contrast, the United States values private-sector sovereignty and the societal benefits of entrepreneurial spirit. In addition, in the United States, privacy may be characterized as harmful to economic interests. This difference in value structure may explain the differences in privacy strategies between the two countries. Moreover, the resulting value structure will depend in part on the power struggle between private industry and consumer protection advocates.[137] Notwithstanding, the highly sensitive nature of patient information resulted in the United States enacting a comprehensive health privacy law.

Finally, a critical reason for the differences in privacy protections for personal medical data stems from the differences in the health care systems themselves. Both the United States and Canada have enacted comprehensive federal privacy legislation aimed at governmental actors. Because many of Canada's governmental services include forms of health care delivery, personally identifiable medical data was naturally included in the mix of privacy protections. By contrast, the federal privacy law covering actions of government actors did not affect the privatized U.S. health care system. Thus, the system of health care delivery in each country has led to a profound difference in privacy protections afforded to medical data.

B. Internet Pharmacy Sales

The United States and Canada primarily regulate the sale of prescription drugs at the federal level.[138] In addition, pharmacies in both Canada and the United States must seek local licenses from each state/province/territory in which they wish to sell prescription medications.

136. The Privacy Act gives the Privacy Commissioner broad powers to investigate individuals' complaints, to launch his own complaint, and to audit federal agencies' compliance with the Act. *See* Privacy Act, R.S.C., ch. P-21, §§ 29, 37(1) (1985) (Can.).

137. An increasing number of corporations favor a federal privacy law over fifty varying state rules. In addition, allowing states to legislate privacy standards could produce obstacles for consumers seeking the benefit of choice of law and forum language included in privacy policies. *See* Declan McCullagh, *Should States Regulate Privacy?*, WIRED NEWS (Feb. 1, 2001), *at* http://www.wired.com/news/politics/0,1283,41511,00.html.

138. *See* 21 U.S.C. § 331 (Supp. IV 1998); Controlled Drugs and Substances Act, S.C., ch. 19 (1996) (Can.), Controlled Drugs and Substances Act, S.C., ch. 19 (1996) (Can.).

1. United States

Licensure to conduct pharmaceutical sales is not currently regulated at the federal level. Instead, licensure is required for each state in which a pharmaceutical company wants to conduct sales.

a. Professional Licensure

All fifty states have laws that regulate the relationship between the patient/consumer and health care professional. For purposes of this Comment, the relevant laws are those that set requirements for licensure of health care professions and penalties for practicing without a license, pharmacy licensure, and accreditation requirements. Additionally, some health care professions may have professional codes of ethics, some of which are enforceable by licensure or ethics boards. For example, the American Medical Association ("AMA") has warned doctors about the need to first "examine" a patient before providing an online prescription.[139]

Every state in the nation requires physicians, psychiatrists, and registered nurses to be licensed by the state in which they practice their profession. Variations exist in the licensure requirements of each state, which can have significant implications for a health-related Web site. Consequently, there is a growing concern over the current licensure system because of Internet and telehealth[140] applications, where state borders are evaporating.

With an eye toward embracing the new electronic age, many options have been proposed for developing a new interstate licensure framework. While these proposals currently apply to health care professionals, they could also apply to organizations selling prescription drugs, such as those engaged in Internet pharmacy sales. For example, the College of American Pathologists proposed a system whereby state boards grant licenses to health professionals in other states that have equivalent standards.[141] An alternative solution is the National Council of State Boards of Nursing program, which is based on a system of general mutual recognition,[142] a

139. *See* Gary Baldwin, *AMA Warns Doctors on Dangers of Web Pill Pushing*, AM. MED. NEWS, July 19, 1999, at 23.

140. Telehealth is defined as the "use of electronic information and telecommunications technologies to support long-distance clinical health care, patient and professional health-related education, public health and health administration." Office for the Advancement of Telehealth, *Welcome*, *at* http://telehealth.hrsa.gov/welcome.htm (last visited Feb. 1, 2001).

141. *See* Joanne Kumekawa, *Telehealth Update, Issue: Licensure Update*, *available at* http://telehealth.hrsa.gov/pubs/licens.htm (last visited Feb. 1, 2001).

142. In November 1998, the National Council adopted an Interstate Nurse Licensure Compact. This Compact created a unified standard for nurses' licenses and gave nurses the ability to practice telemedicine in any state that adopts the Compact. At this time, nine states

concept "in which the licensing authorities voluntarily enter into an agreement to legally accept the policies and processes (licensure) of a licensee's home state."[143] Under mutual recognition, the licensee secures a license in the licensee's home state and need not obtain additional licenses to practice in other states that have also adopted the program.[144] Thus, several solutions can be imagined that both secure state oversight and high standards of licensure and embrace interstate health care delivery.

b. Sale of Prescription Drugs Over the Internet

A recent event highlights the problem of prescription drugs sold over the Internet. In August 2000, a Miami, Florida-based pharmaceutical supply company was charged with conspiring to illegally sell prescription drugs over the Internet.[145] Purportedly, the Web site provided both online and telephone consultations "with real doctors;" however, consumers did not actually receive medical consultations before getting prescriptions.[146] Instead, government officials alleged that an Alabama doctor repeatedly wrote phony prescriptions without any contact with the consumers, and an Alabama pharmacy filled the prescriptions.[147] Officials from the Food and Drug Administration ("FDA") and DOJ said the defendants were indicted for conspiring to sell such drugs as Viagra, Propecia, and Claritin-D to consumers who did not have valid prescriptions.[148]

Although many reputable Internet pharmacies exist today, the FDA is concerned with the public health implications of rogue Web site operators, owners, and affiliates.[149] Such concerns include the sale of prescription drugs without a prescription, the sale of unapproved new drugs, health fraud, and counterfeit medications.[150] While working with state and federal agencies to better coordinate enforcement efforts of illegal online sales and to analyze ways to regulate online sales, the FDA nonetheless maintains that a self-regulatory framework is crucial to the success of online pharmacies.[151] In testimony before the House Commerce Committee, the

have adopted the Compact. *See, e.g.*, UNITED STATES DEP'T OF COMMERCE, TELEMEDICINE REPORT TO CONGRESS 27-50 (1997).

143. *Id.* at 37.

144. *Id.* at 37-38.

145. *Web Drug Site Indicted*, WIRED NEWS (Aug. 7, 2000), *at* http://www.wired.com/news/politics/0,1283,38088,00.html.

146. *Id.*

147. *Id.*

148. *Id.*

149. *See Hearings*, *supra* note 2, at 93-102 (testimony of Janet Woodcock).

150. *Id.*

151. *Id.* at 95.

FDA took the position that "government should encourage private sector leadership in achieving a safe marketplace."[152]

Working under this self-regulatory framework, the U.S. National Association of Boards of Pharmacy ("NABP")[153] has implemented a voluntary certification program in which participating Internet pharmacies must meet state licensing criteria and Verified Internet Pharmacy Practice Site ("VIPPS")[154] criteria. Pharmacies must apply, pay an annual licensing fee, and undergo a site inspection.[155] The VIPPS certification under the NABP requires: compliance with state licensing and inspection in the home state and each state where pharmaceuticals are dispensed; adherence to the patient's right to privacy, authentication, and security; implementation of a recognized quality assurance program; and meaningful consultation between patients and pharmacists.[156] Under this regime, the state pharmacy boards act as one regulatory body.[157] Additionally, former President Clinton announced a plan to require online pharmacies to receive FDA certification before they sell prescription drugs over the Internet.[158]

Furthermore, the AMA has its own set of self-regulatory guidelines governing its Web sites.[159] The goal of AMA's code of ethics is to reduce worries about misleading information and breaches of confidentiality in the online world. The AMA stresses disclosure, informed consent, privacy, and confidentiality, and it places a restriction on inserting advertisements next to online articles on the same topic.[160] These guidelines apply to health information sites, journal articles, and other sources of consumer medical information. Nonetheless, these guidelines do not address online diagnosis and prescription fulfillment without direct patient contact.[161]

Aside from self-regulatory measures, the Federal Food, Drug, and

152. *Id.*

153. The NABP is a professional organization representing state boards of pharmacy in all fifty states. NABP assists state licensing boards in developing, implementing, and enforcing uniform standards to protect the public health. *See* NABP, *Who We Are*, *at* http://www.nabp.net/ (last visited Feb. 1, 2001).

154. VIPPS was developed by NABP in the spring of 1999 as a response to public concern of the safety of pharmacy practices on the Internet. *See* NABP, *VIPPS*, *at* http://www.nabp.net/vipps/intro.asp (last visited Feb. 1, 2001) [hereinafter *VIPPS*].

155. *See* VIPPS, *VIPPS Certification Process*, *at* http://www.nabp.net/vipps/pharmacy/intro.asp (last visited Feb. 1, 2001).

156. *VIPPS*, *supra* note 154.

157. *Id*.

158. *Online Pharmacies: Clinton Proposes Greater FDA Authority over Online Pharmacies; Reactions Skeptical*, 9 Health Law Rep. (BNA) 12 (Jan. 6, 2000).

159. AMA, *Principles Governing AMA Web Sites*, *at* http://www.ama-assn.org/ama/pub/category/1905.html (last visited Feb. 1, 2001).

160. *Id*.

161. *Id*.

Cosmetic ("FDC") Act is currently the primary enforcement mechanism by which the DOJ may protect consumers engaging in the purchase of prescription drugs over the Internet.[162] In establishing the system that currently regulates the sale of prescription drugs, Congress developed a plan that relied on both the physician and the pharmacist to protect patients from knowing or accidental misuses of medicines.[163] Under the FDC Act, drugs that are considered prescription drugs may be distributed only with a valid prescription under the professional supervision of a physician.[164] In addition, the FDC Act prohibits the manufacture of misbranded or adulterated drugs.[165] A prescription drug is considered "misbranded" if it is not dispensed pursuant to a valid prescription in accordance with 21 U.S.C. § 353(b).[166] The FDC Act is also violated when misbranded drugs are distributed or introduced into interstate commerce.[167]

Other enforcement mechanisms for the sale of prescription drugs over the Internet include the Controlled Substances Act,[168] the FTC Act,[169] and federal mail and wire fraud statutes.[170] The Controlled Substances Act prohibits dispensing controlled substances without a valid prescription.[171] As previously mentioned, the FTC Act protects consumers from unfair or deceptive acts or practices. To the extent that an online pharmacy makes false representations about health-related services on its Web site, the FTC Act could be used in a civil enforcement action to eliminate such an unfair or deceptive trade practice. Finally, depending on the facts of a particular case, federal mail and wire fraud statutes could be invoked in either a criminal or civil proceeding anytime an online pharmacy defrauds a consumer using the postal or telecommunications systems.

2. Canada

In Canada, the federal government approves pharmaceutical products, but the individual provinces and territories administer the health care plans, including any pharmacy programs.[172] Currently, it is illegal for Canadian

162. *Hearings*, *supra* note 2, at 87 (testimony of Ivan Fong).
163. *See* 21 U.S.C. § 353(b)(1) (Supp. IV 1998).
164. *Id*.
165. *Id*. § 331(a) (1994).
166. *Id*. § 353(b)(4)(A) (Supp. IV 1998).
167. *Id*. § 331(a) (1994).
168. *See id.* §§ 822, 829, 841.
169. *See* 15 U.S.C. § 45.
170. *See* 18 U.S.C. § 1345 (Supp. IV 1998).
171. *See* 21 U.S.C. § 829(a) (1994).
172. *See* Nat'l Ass'n of Pharmacy Regulatory Auths., *Canada's Pharmacy Regulatory Authorities*, *at* http://www.napra.org/protect/provincial.html (last visited Feb. 1, 2001)

pharmacies to provide prescriptions over the Internet.[173] It is lawful, however, to link an Internet pharmacy with a bricks-and-mortar pharmacy, which locally dispenses the medication.[174] Any licensed pharmacy providing Internet services must meet the standards of practice within its province.[175] Canada's federal enforcement mechanisms for illegal online sales include the Controlled Substances Act[176] and the Food and Drugs Act.[177]

Self-regulatory measures are also prominent in Canada. In 1998, the National Association of Pharmacy Regulatory Authorities ("NAPRA")[178] developed the *Model Standard of Practice for Canadian Pharmacists*, which provides guiding principles for the electronic transmission of prescriptions.[179] NAPRA asked Health Canada to interpret federal legislation to allow for online transmission.[180] In September 1999, NAPRA initiated discussions with the United States NABP to possibly adopt or adapt the VIPPS program for use in Canada.[181] Currently, Canada is making progress toward adopting this or a similar certification program.[182]

IV. CONCLUSION

In the final analysis, the United States and Canadian approaches to protecting an individual's right to privacy and regulating Internet pharmacies do not differ so greatly. The most noticeable difference arises in a general right to privacy in terms of protecting personally identifiable information.

While Canada has recently taken a strong position in doing away with the hodgepodge of privacy laws that govern only specific industries or that simply regulate public actors, the United States is looking primarily toward self-regulatory mechanisms to protect against private-actor invasions of privacy. In addition, the United States maintains a sectoral approach to privacy protections. In one sense, a sectoral approach may provide greater

(citing Canada's individual pharmacy regulatory authorities).

173. Canadian Pharmacists Ass'n, *supra* note 22.

174. *Id.*

175. *Id*.

176. Controlled Drugs and Substances Act, S.C., ch. 19 (1996) (Can.).

177. Food and Drugs Act, R.S.C., ch. F-27 (1985) (Can.).

178. NAPRA, *Formation and Purpose*, *at* http://www.napra.org/about/purpose.html (last visited Feb. 1, 2001). NAPRA is a public-sector association that facilitates the activities of provincial pharmacy regulatory authorities. *Id*.

179. NAPRA, *Model Standards of Practice for Canadian Pharmacists* (Apr. 1998), *at* http://www.napra.org/practice/ standards.html (last visited Feb. 1, 2001).

180. Canadian Pharmacists Ass'n, *supra* note 22.

181. *Id*.

182. *Id*.

privacy protection because of the specificity inherent in legislation geared at a single subject area, and this may be especially beneficial in terms of the highly sensitive nature of personal medical data. Nonetheless, because of the Internet's vulnerabilities and the unknown future for online tracking and profiling, perhaps a baseline framework of privacy standards for all personally identifiable information should be enacted into federal law before consumers lose confidence in the online medium or states enact widely divergent legislation. Restoring public trust in our health care system and providing very specific limits on individually identifiable health information was possibly the reasoning for enacting HIPAA and its Privacy Rule.

Pharmacy sales are highly regulated transactions in both the United States and Canada. Both countries have enacted federal laws that overlay state-, province-, and territory-specific licensure laws. Additionally, both countries face difficult decisions as to how to facilitate and encourage growth in this valuable medium, while at the same time guarding against fraudulent activity. Furthermore, states, provinces, and territories are fond of local licensure and may lodge significant objections to any national solution that infringes upon their sovereignty. Nonetheless, before the Internet pharmacy can realize its full potential and have continuity in operations, there should be a national or mutual recognition approach to local licensure. If implemented thoroughly and with proper oversight, such a program would both energize this valuable medium of pharmaceutical sales and protect consumers in the online world through continued patient-physician contact and examinations.