Loyola of Los Angeles International and Comparative Law Review

Volume 23 | Number 1 Article 2

2-1-2001

Medical Privacy Rights in Anonymous Data: Discussion of Rights in the United Kingdom and the United State in Light of the Source Informatics Cases

Yaron F. Dunkel

NOTES AND COMMENTS

MEDICAL PRIVACY RIGHTS IN ANONYMOUS DATA: DISCUSSION OF RIGHTS IN THE UNITED KINGDOM AND THE UNITED STATES IN LIGHT OF THE *SOURCE INFORMATICS* CASES

I. INTRODUCTION

Privacy is the ability to control knowledge about ourselves.[1] Invasion of privacy occurs when an individual is deprived of the ability, or the autonomy, to preclude unauthorized users from accessing the individual's personal information.[2] Accordingly, a patient's right to privacy is violated when personal medical information is revealed to an unauthorized third party.[3] As this Note discusses, this should hold true even if such information is rendered anonymous by the removal of all data relating to the patient's identity.[4]

Nevertheless, in 1999, a British appellate court held that pharmacists are permitted to make unauthorized use, including disclosure, of anonymous patient data,[5] for *whatever purpose they wish.*[6] The ruling was a result of requests by data-collection companies to purchase information about drugs prescribed to

---

1. Charles Fried, *Privacy*, 77 YALE L.J. 475, 483 (1968).

2. *Id.* at 482–83. "To be deprived of this control not only over what we do but over who we are is the ultimate assault on liberty, personality, and self-respect." *Id.* at 485.

3. *See generally* Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451, 485–89 (1995) (indicating that the proliferation of medical data collection allows access to numerous authorized and unauthorized users, which creates many opportunities for invasion of privacy).

4. *See* discussion *infra* Part VI.

5. R. v. Dep't of Health *ex parte* Source Informatics Ltd., 1 All E.R. 786, 796–97 (C.A. 2000), *rev'g* 4 All E.R. 185 (Q.B. 1999). The data obtained in this case was the physician's name, the date of prescription, the product and the quantity prescribed. *Id.* at 788.

6. According to the appellate court, the central issue was whether the "duty of confidence to patients prevent[s] pharmacists from using the material contained in the [general practitioner's] prescription forms for whatever purposes they wish." *Id.* at 788. It held that the pharmacist is only limited by his or her conscience. *Id.* at 796.

patients.[7] The British Department of Health responded to the purchases by issuing a policy statement to physicians and pharmacists that discouraged the sale of the prescription drug data, even when the data does not identify the patients.[8] The policy stated that "under common law... the general rule is that information given in confidence [by a patient] may not be disclosed without the consent of the provider of the information."[9] The Department of Health warned that any physician or pharmacist "disclosing, prescribing or dispensing information in the way described will be incurring legal risks. On policy grounds, ... [the Department] would strongly discourage *all* such disclosures."[10] The policy guidelines warned that if doctors or pharmacists participated in the data collection plan, they would breach the confidence of the patients.[11]

As a result of the policy statement, general practitioners refused to sell their patients' prescription drug information to the data-collection companies.[12] Physicians that previously agreed to the sale refused to perform on their contracts.[13] Consequently, the policy statement damaged the business of data-collection companies such as Source Informatics Ltd. (Source Informatics).[14]

Source Informatics, claiming that the British Department of Health's policy statement resulted in loss of business,[15] brought suit against the health authorities, seeking to have the policy declared "erroneous in law."[16] In a short-lived landmark decision,[17] the trial court agreed with the Department of Health's policy and denied Source Informatics' request for declaratory

---

7. R. v. Dep't of Health *ex parte* Source Informatics Ltd., 4 All E.R. 185, 187 (Q.B. 1999), *rev'd*, 1 All E.R. 786 (C.A. 2000). The company that prompted the Health Department's policy statement is not the company that filed the court action. 4 All E.R. at 187.

8. 4 All E.R. at 187.

9. *Id.*

10. *Id.* (emphasis added).

11. Cherry Norton, *Sale of Patient Drug Details is Ruled Illegal*, THE INDEP. (London), May 29, 1999, at 10.

12. *Source in Court Battle to Keep Prescription Data*, CHEMIST & DRUGGIST, May 22, 1999, at 32.

13. *Id.*

14. *Id.*

15. *See Source Informatics Ltd.*, 4 All E.R. at 188.

16. *Id.*

17. Jeremy Clay, *Landmark Move on Prescriptions*, LEICESTER MERCURY, June 1, 1999, at 26.

relief (*Source I*).[18] It held that disclosure of anonymous prescription information under Source Informatics' plan was an "unauthorised [sic] use by the pharmacist of confidential information"[19] and, thus, a "clear breach of confidence."[20]

In *Source I*, the court held that *express consent* is always necessary for the disclosure of anonymous drug prescription data to a third party.[21] The ruling created "widespread confusion about how prescription data can be used legally"[22] causing some pharmacy chains to stop collecting prescription data from their branches.[23] As a result, several private British healthcare organizations and the National Pharmaceutical Association intervened in Source Informatics' appeal[24] to seek clarification on how pharmacies may use prescription data to run their business.[25] The appellate court reversed the trial court's decision that granted broad patient privacy rights in situations when the data cannot identify the patient (*Source II*).[26]

Like the United Kingdom, the United States recognizes a right to privacy established by case and statutory law.[27] This right, however, is not absolute[28] and has not been extended to medical information revealed to pharmacists,[29] nor to non-identifying medical data.[30] Accordingly, despite U.S. federal and state attempts to safeguard medical privacy, such protection has only

---

18. Source Informatics Ltd., 4 All E.R. at 198.

19. *Id.* at 192.

20. *Id.*

21. *See Source Informatics Ltd.*, 4 All E.R. at 192–93; *see also* Lisa Thomlinson & Abha Thakor, *GMC Admits Confidentiality Rules in Doubt*, PULSE, July 10, 1999, at 1. Source Informatics did not contend that a patient gives implied consent to a physician or pharmacist for the sale of the information to a third party. The court, therefore, did not consider nor did it find it necessary to consider this possibility. *Source Informatics Ltd.*, 4 All E.R. at 192–93. The trial court, however, recognized that implied consent may exist in situations where the physicians and pharmacists *themselves* use the anonymous information for medical research and advancement. *Id.*

22. *NPA to Intervene in Source Informatics Appeal Court Hearing*, CHEMIST & DRUGGIST, Sept. 25, 1999, at 36.

23. *Id.*

24. *Source Informatics Ltd.*, 1 All E.R. at 787.

25. *NPA to Intervene in Source Informatics Appeal Court Hearing*, supra note 22, at 36.

26. 1 All E.R. at 801.

27. *See* discussion *infra* Part IV.

28. United States v. Westinghouse Elec. Corp., 638 F.2d 570, 578 (3d Cir. 1980).

29. Gostin, *supra* note 3, at 510; Evans v. Rite Aid Corp., 478 S.E.2d 846, 848 (S.C. 1996).

30. *See* discussion *infra* Part IV.A.3.

been afforded to identifiable medical information.[31] Thus, the laws in the United States expressly permit the use of anonymous data.[32]

This Note discusses the United Kingdom's protection of personal medical information, in light of the *Source I* and *II* decisions and the significance of the United Kingdom's short-lived attempt to broaden patient's medical privacy rights. In addition, it analyzes the United States' reluctance to protect patient medical data from misuse.[33] It argues that medical privacy should protect patients' records from access by unauthorized third parties, and give patients a private cause of action when their records are misused without sufficient public policy justifications.[34] Furthermore, it concludes that an individual's privacy right should also extend to anonymous medical information.[35] This right to confidentiality, moreover, should not only pertain to information revealed to physicians, but to other healthcare professionals, such as pharmacists.[36]

Part II of this Note begins by defining privacy as a right to autonomy. Part III discusses the *Source I* and *II* decisions and their impact in the United Kingdom. Part IV examines medical privacy rights in the United States, considers steps that have been taken to extend those rights, and explores unprotected areas. Part V establishes that, aside from the *Source I* case, the limited medical rights in the United Kingdom and the United States involve identifiable data, and do not protect anonymous data that is widely used in medical research. Part VI concludes that in the absence of important public policy concerns, courts should recognize that the right to privacy is breached when a health care professional uses anonymous medical data for purposes for which the patient did not consent.

---

31. *See* discussion *infra* Part IV.

32. *See id.*

33. *See* Michael P. Roch, *Filling the Void of Data Protection in the United States: Following the European Example*, 12 SANTA CLARA COMPUTER & HIGH TECH. L.J. 71, 88 (1996).

34. *See* discussion *infra* Part VI.

35. *Id.*

36. *Id.*

II. THE RIGHT TO PRIVACY

"Privacy is not simply an absence of information about us in the minds of others; rather it is the *control* we have over information about ourselves."[37] Privacy, therefore, is not simply the protection of identity—it is a person's ability to control access to information about oneself.[38] Privacy is required to ensure an individual's sense of respect, love, friendship, and, most important to the purpose of this Note, trust.[39]

Because an individual's medical records are "intensely personal,"[40] when a patient gives prescription information to a pharmacist and is unable to control how the information, albeit anonymous, is used, that patient's sense of privacy is invaded. The patient lost the "ability to retain autonomous decision-making authority" over the use of the data.[41] The patient permitted the information to be used only to fill a prescription, not to aid pharmaceutical companies in marketing drugs.[42] Because privacy is the right to control information,[43] a patient should not lose that right simply because the information is made anonymous.

III. A SHORT WINDOW OF SUBSTANTIAL PATIENT PRIVACY IN THE UNITED KINGDOM

A. An Analysis of The Lower Court's Decision in Source I

In *Source I*, the trial court created a private cause of action for breach of confidence against pharmacists and physicians who disclose medical records to private companies for commercial

---

37. Fried, *supra* note 1, at 482.

38. *Id.*; Lawrence O. Gostin et al., *Privacy and Security of Health Information in the Emerging Health Care System*, 5 HEALTH MATRIX 1, 3 (1995) ("[P]rivacy rights are widely understood as the right of an individual to limit access by others to some aspect of the person.").

39. Fried, *supra* note 1, at 477–83. Trust is important because the court in *Source I* based its holding on the principle that a patient must be able to maintain trust in the healthcare provider. R. v. Dep't of Health *ex parte* Source Informatics Ltd., 4 All E.R. 185, 195–96 (Q.B. 1999), *rev'd*, 1 All E.R. 786 (C.A. 2000).

40. David L. Wheeler, *Is the Loss of Personal Privacy the Price of Medical Progress?*, THE CHRON. OF HIGHER EDUC., Sept. 17, 1999, at A21.

41. Gostin et al., *supra* note 38, at 20.

42. R. v. Dep't of Health *ex parte* Source Informatics Ltd., 4 All E.R. 185, 189 (Q.B. 1999), *rev'd*, 1 All E.R. 786 (C.A. 2000).

43. Fried, *supra* note 1, at 483.

use.[44] The ruling was a surprise because the United Kingdom has been slow to protect its citizens' privacy.[45]

Until the *Source I* ruling, the healthcare community believed that removing all identifying patient information satisfied the legal requirements for confidentiality.[46] Companies like Source Informatics believed they could collect anonymous prescription data from pharmacists by downloading it into a database without risking breach of confidentiality liability.[47] The data included the name of the physician as well as the identity and quantity of the prescribed drugs, but did not include any information that identified the patient.[48] Source Informatics sold the data to pharmaceutical companies who, in turn, used the database to target physicians with promotions and products.[49]

Additionally, physicians were able to disclose anonymous records to third parties. Shortly before the ruling in *Source I*, the General Medical Council (GMC) drafted policy guidelines that allowed British physicians to obtain implied consent from patients to disclose records for financial and clinical audit, post-payment verification, and medical research by placing posters and leaflets in the waiting room.[50] The guidelines were based on the view that information that is anonymous and aggregated could be used without raising a question of confidentiality.[51] Some scholars, however, asserted that "[s]imply putting a sign up in the pharmacy saying that information might be passed on [to others] would not count as having informed consent . . . ."[52] Following *Source I*, on the advice of the Queen's Counsel that the guidelines would

---

44. *Source Informatics Ltd.*, 4 All E.R. at 198.

45. *See* Sir Thomas Bingham, *It's the Tort that Counts*, THE OBSERVER, May 27, 1996, at T16 (noting that in the United Kingdom, there is "no recognition of a general right to privacy.").

46. *In the News this Month: In the Pharmacy World*, COMMUNITY PHARMACY, July 1999, at 3 [hereinafter *Pharmacy World*].

47. R. v. Dep't of Health *ex parte* Source Informatics Ltd., 1 All E.R. 786, 788 (C.A. 2000), *rev'g* 4 All E.R. 185, 187 (Q.B. 1999). Source Informatics paid for this prescription information by donating a nominal fee to a charity of the pharmacist's choice. 1 All E.R. at 788.

48. *Prescription Information Remains Confidential*, THE TIMES (London), June 14, 1999, at 45.

49. *Source in Court Battle to Keep Prescription Data, supra* note 12, at 32.

50. Thomlinson & Thakor, *supra* note 21, at 1.

51. Linda Beecham, *Medicopolitical Digest: GMC Delays Guidelines on Confidentiality*, BRIT. MED. J., Sept. 25, 1999, at 858.

52. *Make Sure of Security Needs*, CHEMIST & DRUGGIST, Sept. 25, 1999, at 21.

violate the court's ruling, the GMC decided to postpone the publication of its guidelines pending the result of Source Informatics' appeal.[53]

1. Non-Identifying Information Was Held to Be Confidential

After its unsuccessful attempt to persuade the Department of Health to change its policy,[54] Source Informatics asked the trial court (*Source I*) to declare: 1) that the guidance contained in the policy document was erroneous in law and 2) that anonymous information disclosed by physicians and pharmacists to a third party is not a breach of confidence.[55]

The trial court defined breach of confidence as: (1) the disclosure of confidential information that is inaccessible to the public, (2) under circumstances that impose an obligation on the recipient to respect the confidentiality of the information and (3) that is breached by the recipient.[56] In *Source I*, the court agreed with the Department of Health that when a patient explicitly or implicitly gives medical information for a limited purpose, this consent imposes upon the recipient a duty to refrain from using the information for any other purpose.[57] The duty applies not only to the recipient, but also to any third party that receives the information thereafter.[58] A patient can show a breach of duty by demonstrating that the recipient made an unauthorized use of the information for a purpose other than that for which it was given.[59]

Source I centered on two issues. First, whether the disclosure of non-identifying information to a third party is an unauthorized use of the data, which would satisfy the third element for breach of

---

53. Beecham, *supra* note 51, at 858.

54. R. v. Dep't of Health *ex parte* Source Informatics Ltd., 4 All E.R. 185, 188 (Q.B. 1999), *rev'd*, 1 All E.R. 786 (C.A. 2000).

55. 4 All E.R. at 188.

56. *Id.* at 190–91 (citing FRANCIS GURRY, BREACH OF CONFIDENCE 3–5 (1984)). In this case, the authorized recipients of the patient information are physicians and pharmacists. *See generally id.*

57. *Id.* at 190 (citing GURRY, *supra* note 56, at 3).

58. *Id.* Therefore, a data collection company that obtains medical information from a physician or pharmacist, who breached the duty to a patient, will itself be in breach. Hence, both the healthcare providers and the data collection company could be sued for breach of the duty of confidence. *See id.*

59. *Id.* at 190–91.

confidence.[60] Second, whether a patient must show detriment to state a cause of action.[61]

Source Informatics argued that the disclosure of anonymous data to third parties is not a breach of confidence because the data loses its confidential nature when the individual's identifying information is removed.[62] According to Source Informatics, only use of information containing identifying data amounts to breach of confidence.[63] It argued that because the company uses the data only after it becomes anonymous, at which point it loses its confidential character, the patient's confidence is not breached.[64] The trial court, however, rejected Source Informatics' suggestion that the process of disclosing information can be divided into two stages: (1) making the information anonymous and thus non-confidential and then (2) using the data.[65] Instead, according to the trial court, the disclosure of patient medical data immediately becomes a "clear breach of confidence unless the patient gives consent."[66] Therefore, the *Source I* court held that pharmacists who disclose any data without the patient's consent would expose themselves to successful actions for breach of confidentiality.[67]

2. Disclosure of Anonymous Data Was Held to Be Detrimental as a Matter of Public Policy

The *Source I* court then considered whether detriment is a necessary element of breach of confidentiality and, if so, what type of unauthorized use of the information is detrimental to the patient.[68]

The court first determined that detriment remains a necessary part of breach of confidence.[69] Breach of a patient's confidence may be defined as the loss of privacy when "others obtain information about an individual, pay attention to him[,] or gain access to him."[70] Under this definition, an individual patient

60. *See id.* at 192.
61. *See id.* at 192–94.
62. *Id.* at 192.
63. *Id.*
64. *Id.*
65. *Id.*
66. *Id.*
67. *Id.* at 197.
68. *Id.* at 191, 193–94.
69. *See id.* at 194.
70. *Id.* at 195.

would not suffer detriment from the use of *anonymous* data.[71] While most patients would not be concerned that statistical information is extracted from their prescription records,[72] for others, any non-consensual use of their records is unconscionable.[73] Accordingly, because pharmacists provide a service to the general public and must retain its trust,[74] the trial court found that it is in the public interest to keep such information private so that no patients are inhibited from seeking medical care.[75] Therefore, a pharmacist who breaches the patient's confidence by publicizing anonymous data might cause enough detriment to justify a remedy.[76]

The trial court noted, however, that its decision might not apply when a sufficient public interest exists so as to justify making the information available to others without the patients' consent.[77] But Source Informatics did not argue that the public would benefit from the sale of the prescription data.[78] Nor did it argue that the patients gave the health care providers their implied consent, as may be the case when physicians use anonymous information for "research, medical advancement, or the proper administration of the service."[79] Instead, it argued that the anonymous information has commercial value. The trial court did not find this argument persuasive enough to overcome the public interest in the protection of confidence.[80]

The Department of Health, on the other hand, argued that the unauthorized use would not advance the public interest.[81] It claimed that the sale would inhibit patients who greatly value their privacy from seeking medical assistance if they feared that

---

71. *Id.*
72. *Id.*
73. *Id.*
74. *Id.* at 196.
75. *Id.* (finding, however, that a breach of confidence may be acceptable if it is in the public interest).
76. *Id.* at 197 (stating that "breach of confidence in itself might carry with it sufficient detriment to justify the grant of a remedy."). *See also id.* at 196–97 (citing *X v. Y*, 2 All E.R. 648, 657–58 (Q.B. 1988) (holding that detriment in the use of information in a way that does not identify the patient or the health care provider does not preclude legal relief)).
77. *Id.* at 196
78. *Id.*
79. *Id.* at 192.
80. *Id.* at 196.
81. *Id.*

pharmacists would make their data available to unauthorized parties; Judge Latham accepted this argument.[82] In addition, the Department of Health suggested that the data obtained by Source Informatics and used by pharmaceutical companies for target marketing would affect the prescribing habits of physicians and substantially increase the costs of health care.[83]

B. Losing Confidentiality Rights and Returning to the Past: The Court of Appeals Allows the Sale of Unauthorized Anonymous Information

As a result of the decision in *Source I* and the Department of Health's policy that the use of anonymous data would not obviate a breach of confidence,[84] for a brief period of time privacy rights in the United Kingdom expanded. To avoid an action for breach of confidence, physicians and pharmacists were required to obtain patient consent.[85]

When the Department of Health issued its policy statement, it recognized that the public interest in disclosure could outweigh the privacy interest of the patient, but doubted that use of medical data for pecuniary purposes would be in the public interest.[86] It suggested, instead, that such disclosure would be directly contrary to public interest.[87] The trial court accepted the Department's argument when it found that the patient's data must be protected to guard the public's trust in the profession.[88]

On appeal, however, the *Source II* court rejected the Department's argument and reversed the trial court's ruling.[89] It found that the general duty of confidence does not prevent pharmacists from selling data in any way they find conscionable so

---

82. *Id.*

83. R. v. Dep't of Health *ex parte* Source Informatics Ltd., 1 All E.R. 786, 789 (C.A 2000) *rev'g* 4 All E.R. 185 (Q.B. 1999).

84. *Source Informatics Ltd.*, 4 All E.R. at 187.

85. *Id.* at 192.

86. *Id.* at 187.

87. *Source Informatics Ltd.*, 1 All E.R. at 789 .

88. *Source Informatics Ltd.*, 4 All E.R. at 196. The appellate court, however, noted that the Department of Health was primarily concerned with potential rise in medical costs due to use of the data to market prescription drugs. *Source Informatics Ltd.*, 1 All E.R. at 789.

89. *Source Informatics Ltd.*, 1 All E.R. at 797 (holding that the pharmacist's duty of confidence is not breached by the sale of the anonymous data).

long as the patients' anonymity is fully protected.[90] This holds true regardless of whether the patient would object to such use.

In *Source II*, the court accepted the trial court's definition of breach of confidence as consisting of three elements.[91] The information must: (1) have an element of confidence, (2) be obtained under circumstances requiring that confidence be kept, and (3) be used without authority to the detriment of the patient.[92] Nevertheless, unlike the trial court, the court of appeals struck down the Department's policy, finding that the third element was not satisfied.[93] The appellate court dismissed as "unreal" the Department's argument that the information was disclosed to a pharmacist only for the limited purpose of dispensing drugs and that any other use of it, even if kept anonymous, is an objectionable misuse.[94] It reasoned that because the patient's autonomy to protect his or her *identity* forms the basis for the patient's interest in the information, the use of the prescription information in a manner that protects the patient's identity would not undermine that patient's interest.[95] Thus, in *Source II*, the appellate court rejected the trial court's finding that the public's distrust of the medical profession for selling anonymous patient data for commercial gain to be a sufficient detriment to the patient.[96] It held that there could be no detriment absent the actual disclosure of the identity of the patient.[97] The fact that a reasonable person would believe that the information is given in confidence is sufficient to create a duty of privacy, but is not sufficient to prohibit all manners of use of that information.[98]

---

90. *Id.* at 796–97 ("[T]he confidant is placed under a duty of good faith to the confider and the touchstone by which to judge the scope of his duty and whether or not it has been fulfilled or breached is his own conscience, *no more and no less*.") (emphasis added).

91. *See id.* at 790. For a general discussion by the trial court of the three elements see *Source Informatics Ltd.*, 4 All E.R. at 190–91.

92. *Source Informatics Ltd.*, 1 All E.R. at 790 (analyzing the issue of detriment, as discussed by the trial court, as part of the third element).

93. *Id.* at 797 (finding that the patient's integrity is not undermined when the data is sold to an unauthorized third party).

94. *Id.* at 796.

95. *Id.* at 797.

96. *See id.* at 796–97 (holding that the issue is not of detriment, but whether a reasonable pharmacist would find the particular use of the data objectionable).

97. *Id.* ("[I]n a case involving personal confidences[,] I would hold . . . that the confidence is not breached where the confider's identity is protected.").

98. *Id.* at 793 (citing Smith Kline & French Labs. (Austl.) Ltd. v. Sec'y to the Dep't of Cmty. Servs. and Health (1991) 99 A.L.R. 679, 691–92. (quoting Moorgate Tobacco Co. v. Phillip Morris Ltd. 56 A.L.R. 193, 203 (1984) (holding that the obligation to maintain

Accordingly, if the information is rendered anonymous, the patient will not suffer any detriment upon disclosure and therefore cannot sue for breach of privacy even when the information is made public.[99]

According to the appellate court, the test for determining whether the use of confidential information violates the patient's right to privacy is whether "a reasonable pharmacist's conscience [would] be troubled by the proposed use to be made of the patient's prescription."[100] Therefore, the appellate court's test is an objective, physician-centered test, rather than the trial court's subjective, patient-centered test.[101] Unlike the trial court, the appellate court was not concerned with whether the patient would distrust the medical community, nor that the pharmacist has a duty to use private prescription information exclusively for the purpose of dispensing drugs.[102] As long as a reasonable pharmacist would not be troubled by the release of the information to a data collection company, the duty of confidence is not breached.[103]

The appellate court specifically held that a patient has no privacy rights when medical data is anonymous, even in the absence of any policy interest to make such data available.[104] The court presumed that privacy could be guaranteed by the data collection company.[105] The appellate court reasoned that as long as the patient is ensured anonymity, the patient has no property interest or proprietary claim in the prescription information, and thus has no right to control its use.[106]

---

confidences "lies in the notion of an obligation of conscience arising from the circumstances in or through which the information was communicated or obtained"))).

99. 1 All E.R. at 797.

100. *Id.* at 796.

101. This suggests that regardless of whether a policy exists for making the data public, a patient who is troubled by such use has no cause of action for breach of confidence.

102. *See* 1 All E.R. at 797.

103. *Id.*

104. *Id.* (holding that the patient has no right to control the use of medical data as long as his or her identity is not revealed).

105. *Id.* at 789.

106. *Id.* at 797.

C. A Patient Who is Denied Privacy Rights in Anonymous Data is Susceptible to Substantial Invasion by the Medical Community

The medical community makes substantial use of anonymous medical data.[107] Several countries, including the United Kingdom, have fashioned policies regarding the right of medical professionals to sell or provide patients' medical records to third parties.[108] For example, in Iceland, the Parliament granted a U.S. biotechnology company based in Delaware an exclusive license to build an electronic database of the country's medical records, including diagnoses, test results, treatments, and side effects.[109] The company used the information along with genetic and genealogical data for commercial purposes,[110] entering into a non-exclusive agreement with Hoffman-La-Roche, Inc.,[111] that provides access to the database, and allows Hoffman-La-Roche to research the genetic origins of twelve common diseases.[112] Although Icelanders may exclude themselves from the database at any time, there is concern that the average Icelander may not be aware of all potential present and future uses of the database.[113] Iceland exemplifies the lack of medical privacy that residents of many countries face.

As a result of the ruling in *Source II*, British healthcare professionals can use anonymous data, including genetic data, in a manner comparable to that in Iceland.[114] Such broad use of anonymous medical information would be upheld under the appellate court's standard if a medical professional would not find

---

107. *E.g.*, Wheeler, *supra* note 40, at A21 (stating that medical knowledge comes largely from the study of medical records, including anonymous records).

108. *See, e.g.*, *Ontario Pharmacists Can Sell Information, Body Says (Ontario College of Pharmacists)*, CANADIAN PRESS NEWSWIRE, May 9, 1996, *available at* LEXIS, News Library, Allnws File (stating that the governing body for Ontario's pharmacists allows its members to sell the *anonymous* prescription information, although the national association for pharmacists' code of ethics condemned the practice and was protested by Ontario doctors).

109. Ruth Chadwick, *The Icelandic Database—Do Modern Times Need Modern Sagas?*, 319 BRIT. MED. J. 441, 441 (1999).

110. *Id.*

111. *Id.*

112. *Id.*

113. *Id.* at 443.

114. *See* R. v. Dep't of Health *ex parte* Source Informatics Ltd., 1 All E.R. 786, 786, 797 (C.A. 2000), *rev'g* 4 All E.R. 185 (Q.B. 1999).

such use unconscionable.[115] The general public, however, finds such use of anonymous medical data reprehensible.[116] For instance, in a 2000 U.S. Gallup Poll, ninety-three percent of persons polled indicated that researchers should not be allowed to study genetic information without the patient's consent.[117]

IV. THE UNITED STATES AFFORDS LIMITED PRIVACY PROTECTIONS

A. Federal Law Provides Insufficient Protection of Medical Data Privacy

Currently, U.S. residents have never been more sensitive about their privacy rights nor more aware of the potential for abuse of their private information.[118] Disclosure of health records, which contain substantial private information, including financial and employment data, indications of disabilities, problems with mental health, and history of disease, as well as sexual and lifestyle information,[119] could result in patient stigmatization, thus discouraging many from divulging sensitive information to their healthcare providers.[120] Accordingly, without adequate privacy protections, patients may lose trust in the medical profession, leaving the integrity of the healthcare system as a whole at risk.[121]

1. The U.S. Courts Recognize a Constitutional Right to Privacy

In *Olmstead v. United States*,[122] Justice Brandeis first articulated that the U.S. Constitution protects the right to be let alone as "the most comprehensive of rights and the right most

---

115. *See* 1 All E.R. at 796.

116. *See generally* THE GALLUP ORGANIZATION, PUBLIC ATTITUDES TOWARD MEDICAL PRIVACY (2000), http://www.forhealthfreedom.org/Gallupsurvey/ (last visited Jan. 1, 2001).

117. *Id.* at 4. The question posed was: *"Should medical and government RESEARCHERS be allowed to STUDY your genetic information (for example, to identify genes thought to be associated with various medical conditions) without first obtaining your permission, or do you feel they should first obtain your permission?"* *Id.* at 17.

118. Paul A. Lombardo, *Genetic Confidentiality: What's the Big Secret?*, 3 U. CHI. L. SCH. ROUNDTABLE 589, 589 (1996).

119. Gostin, *supra* note 3, at 490.

120. *Id.* at 490–91.

121. *Id.* at 490.

122. 277 U.S. 438 (1928).

valued by civilized men."[123] Since then, U.S. courts have recognized that the right to privacy is one of the most "fundamental and cherished rights."[124] The right to privacy includes the individual interest in avoiding unconsented disclosure of personal information.[125] The collection, recording, and dissemination of individualized medical information threatens that right.[126] Consequently, much of the public, congressional, and judicial concern has been with governmental accumulation of medical information and its use in ways that may be detrimental to individual privacy.[127]

2. Federal Case Laws Limit the Right to Privacy

The constitutional right to privacy is not absolute.[128] The U.S. Supreme Court has not formulated a general approach to identifying justifiable privacy rights.[129] Once specific rights are recognized, the Court weighs the individual's recognized privacy interests against the state's interest to determine whether to provide protection.[130] The Supreme Court, therefore, has limited the federal constitutional protection of privacy interests by balancing them against the government's interests.[131]

In *United States v. Westinghouse Electric Corp.*,[132] the Third Circuit Court of Appeals identified seven factors that a court must consider in determining whether the right of personal privacy outweighs the public interest in accessing the information in the context of medical data privacy: (1) the type of records requested; (2) the information the records have or might contain; (3) the safeguards available to prevent subsequent disclosures to others; (4) the potential of harm that subsequent unauthorized disclosure would have; (5) the injury that the disclosure would have on the relationship that compiled the information; (6) the degree of need

123. *Id.* at 478 (Brandeis, J., dissenting).
124. *E.g.*, United States v. Westinghouse Elec. Corp., 638 F.2d 570, 576 (3rd Cir. 1980).
125. *Id.* at 577.
126. *Id.* at 576–77.
127. *Id.* at 576.
128. *Id.* at 578.
129. Susan Clement et al., Note, *The Evolution of the Right to Privacy After Roe v. Wade*, 13 AM. J.L. & MED. 368, 381 (1987).
130. *Id.*
131. Gostin, *supra* note 3, at 495.
132. *Westinghouse*, 638 F.2d at 578.

for access; and (7) the existence of a recognizable public interest in the information.[133]

In *Westinghouse*, the Third Circuit allowed a government agency that was responsible for establishing occupational safety and health standards to subpoena Westinghouse's employees' medical records.[134] Although the court recognized that an employee's medical records are entitled to protection,[135] when the societal benefit in disclosure outweighs the privacy interest, disclosure may be compelled.[136] The court found that the societal interest in protecting the health of employees and the public at large from toxic exposure was substantial.[137] Most significantly, rather than presuming that such intrusion into employee privacy is severe or could harm employee interests, the court placed the evidentiary burden on the company claiming invasion of privacy.[138] A person who wants to avoid disclosure of personal medical information, therefore, has the burden to show that the information should not be disclosed.

Even when the public interest outweighs the right of privacy, disclosure of medical records would be improper if the government lacks "effective provisions for security of the information against subsequent unauthorized disclosure."[139] The threshold of "effective" security, however, is not strict. Relying on earlier cases, the Third Circuit noted that it is sufficient that the government has "adequate" provisions in place to secure the privacy of the information from further unauthorized disclosure.[140] The precautions must be substantial but "not foolproof."[141] The

---

133. *Id.*

134. *Id.* at 570. Westinghouse was under investigation for exposing its employees to significant levels of toxic materials, which caused allergic reactions in some employees. *Id.* at 572.

135. *Id.* at 577 ("There can be no question that an employee's medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection.").

136. *Id.* at 578.

137. *Id.* at 579.

138. *See id.*

139. *Id.*

140. *Id.* at 580 (citing Whalen v. Roe, 429 U.S. 589 (1977) (permitting the state to compile database of names and addresses of patients who obtained by prescription certain legal drugs for which there is also an illegal market); Schachter v. Whalen, 581 F.2d 35 (2d Cir. 1978) (validating the constitutionality of a New York statute allowing the Executive Secretary of New York State Board for Professional Medical Conduct the power to subpoena private patient information, despite the patient's opposition)).

141. *Westinghouse*, 638 F.2d at 580 (citing *Schachter*, 581 F.2d at 37 n.2).

court nonetheless did not discuss what minimal provisions are adequate to ensure confidentiality.

These cases, which provide patients with some medical privacy, dealt only with government's intent to obtain confidential information about identifiable persons. When the information is collected and published in statistical form such that the person cannot be identified, the constitutional right of privacy is not implicated.[142]

3. Federal Privacy Statutes Do Not Protect Unconsented Use of Anonymous Data

In addition to privacy protections afforded by case law, federal statutes provide limited protection against the intrusion into patients' records held by the government. For example, the Freedom of Information Act[143] (FOIA) requires federal agencies to release requested information held in government files, unless the information consists of medical records.[144] The statute requires that all records of federal agencies be made accessible to the public and places the burden on the agency to show that the documents should not be released.[145] The FOIA further requires a government agency to permit public access to any portion of an open meeting.[146] To protect private records from public scrutiny, the Act contains nine exemptions.[147] One of the exemptions has been used to prevent public access to personal medical records.[148] But the U.S. Supreme Court held that a federal agency that

142. United States v. Little, 321 F. Supp. 388, 392 (D. Del. 1971).

143. Freedom of Information Act, 5 U.S.C. § 552 (1994).

144. *See id.* at § 552b(b)–(c).

145. *See* Jean F. Rydstorm, Annotation, *Scope of Judicial Review Under Freedom of Information Act (5 U.S.C. § 552(a)(3)), of Administrative Agency's Withholding of Records*, 7 A.L.R. FED. 876, 881 (1971). In practice, though, courts often require the party seeking disclosure to present some evidence that the agency is improperly withholding the documents sought, before shifting the burden to the agency. *Id.*

146. Freedom of Information Act § 552b(b) ("[E]very portion of every meeting of an agency shall be open to public observation.").

147. *Id.* § 552b(c)(1)–(10)

148. *Id.* § 552(b)(6) (exempting any government records from disclosure that contain "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy"); *see also* E.E. Mazier, *Local Agencies Must Disclose Redacted Versions of Federal Housing Assistance Contracts*, NEW JERSEY LAW., July 8, 1996, at 32 (noting that the exemption applies to medical records).

maintains records merely has the discretion, not the duty, to withhold disclosure.[149]

The Privacy Act of 1974[150] (Privacy Act) provides no more privacy protection for individuals about whom the government collects data than does the FOIA.[151] Congress enacted the Privacy Act simply to ensure that federal agencies use fair information practices in collecting, using, or disseminating records,[152] and specifically to protect "medical history" records.[153] It was not intended to interfere with the right of the public to obtain information contained in federal agency records.[154] Under the Privacy Act, agencies cannot disclose any information to other agencies or individuals without the person's consent.[155] That restriction, however, is subject to several rather broad exceptions.[156] These exceptions include allowing disclosure: (1) to other agency employees who need the record for the performance of their duties or for routine use, (2) to a person showing compelling circumstances involving health or safety, or (3) to a consumer reporting agency.[157] Moreover, any recipient may obtain information if sought for statistical research and the record is *not identifiable*.[158] Like FOIA, there is no invasion of privacy if the collector deletes any identifying characteristics.[159] Furthermore, the Privacy Act does not affect most non-federal agencies that collect health information.[160]

Evidently, Congress is less concerned with anonymous medical information because once the data has been stripped of all identifying information, it leaves no means to associate the information with a specific patient, and therefore poses the fewest privacy concerns.[161] Such data, however, does have the potential

---

149. Gostin, *supra* note 3, at 502–03, (citing Chrysler Corp. v. Brown, 441 U.S. 281, 293 (1979) ("Congress did not design the FOIA exemptions to be mandatory bars to disclosure.")).

150. Privacy Act of 1974, 5 U.S.C. § 552a (1974).

151. *See* Gostin, *supra* note 3, at 500–01.

152. *Id.* at 499–500.

153. Privacy Act of 1974 § 552a(a)(4).

154. Gostin, *supra* note 3, at 501.

155. Privacy Act of 1974 § 552a(b).

156. *Id.*

157. *Id.* § 552a(b)(1)–(12); s*ee also* Gostin, *supra* note 3, at 500 n.224.

158. Gostin, *supra* note 3, at 500 n.224.

159. Dep't of the Air Force v. Rose, 425 U.S. 352, 381 (1976).

160. Gostin, *supra* note 3, at 500–01.

161. *Id.* at 519.

of identifying a racial or ethnic group and painting it in an offensive or misleading light.[162]

Additionally, although the U.S. federal government provides more stringent confidentiality standards for drug and alcohol treatment records,[163] even those do not provide adequate protection. For example, while records of federally funded drug or alcohol treatment facilities usually may only be disclosed with the patient's consent, consent is not required for medical research purposes.[164] In addition, medical records in non-federally funded facilities are not protected.[165]

B. State-Recognized Right of Privacy Does Not Protect Anonymous Data

1. State Statutes Provide Limited Protection of Medical Data

As U.S. federal privacy laws do not affect private actions,[166] Congress left the states to provide protection from private actors.[167] State laws protecting the privacy of medical information vary and contain numerous exceptions, yet the effectiveness of laws in protecting medical information in practice is unknown.[168] Laws protecting the confidentiality of genetic information are an example.[169]

In Colorado, information derived from genetic testing is privileged and cannot be released to unauthorized parties without the written consent of the test subject.[170] The law, however, provides numerous exceptions, including allowing the release of *anonymous* information to research facilities.[171] In Georgia, genetic information for civil use is the unique property of the

---

162. *Id.* at 520–21 (noting that data indicating a disproportionately high rate of HIV infection, mental illness, or alcoholism in discrete populations may lead to adverse effects).

163. Gostin, *supra* note 3, at 503.

164. *Id.* at 503 n.254.

165. *Id.* at 503.

166. Christina M. Rackett, Note, *Telemedicine Today and Tomorrow: Why "Virtual" Privacy is Not Enough*, 25 FORDHAM URB. L.J. 167, 181 (1997).

167. *Id.*

168. Lombardo, *supra* note 118, at 589.

169. *See* GA. CODE ANN. § 33-54-1 (1996); COLO. REV. STAT. § 10-3-1104.7 (1994).

170. COLO. REV. STAT. § 10-3-1104.7(3)(a); *see* Lombardo, *supra* note 118, at 604.

171. COLO. REV. STAT. § 10-3-1104.7(5); *see* Lombardo, *supra* note 118, at 604.

patient.[172] The law, however, explicitly allows use of information derived from genetic testing for scientific research without the patient's consent as long as the patient's identity is not disclosed to third parties.[173] Some states provide disease-specific privacy protection, such as statutes that protect the privacy of people with HIV.[174] Some of these statutes give near-absolute protection and prohibit any disclosure without the patient's consent.[175] Other states, however, provide many exceptions in favor of disclosure, which greatly dilute patients' privacy rights.[176]

2. Limited Protection for Identifiable Information: U.S. Tort and Contract Case Law

In absence of a statute mandating or permitting disclosure, tort and contract law provides patients with limited privacy protection.[177] Recent case law protects various "reasonable expectation[s] of privacy" from unexpected intrusion.[178] U.S. courts, however, have failed to provide substantial protection for the confidentiality of patients' medical records. State courts provide some protection by recognizing a duty of privacy and of confidentiality in tort as well as a contractual duty of privacy.[179] These duties, however, have been applied primarily to physicians and similar health-care providers,[180] not to pharmacists.[181]

The Restatement (Second) of Torts section 652D describes an invasion of privacy as publicizing "a matter concerning the private life of another"[182] that "(a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."[183] According to the Restatement, there is no invasion of privacy if the information was communicated to a specific small

---

172. GA. CODE ANN. § 33-54-1(1); *see* Lombardo, *supra* note 118, at 605.

173. Lombardo, *supra* note 118, at 605 (leading the federal commission to endorse special treatment for AIDS-related medical information).

174. *Id.* at 592.

175. *See id.*

176. Gostin, *supra* note 3, at 508.

177. Roch, *supra* note 33, at 92–93.

178. *See, e.g.*, Sanders v. Am. Broad. Cos., 20 Cal. 4th 907 (1999) (protecting conversations between employees in an employees-only area of an office from secret videotaping).

179. Gostin, *supra* note 3, at 508–09.

180. *See id.* at 509.

181. Evans v. Rite Aid Corp., 478 S.E.2d 846, 848 (S.C. 1996).

182. RESTATEMENT (SECOND) OF TORTS § 652D (1977).

183. *Id.* § 652D(a)–(b).

group, rather than the general public.[184] Some courts, however, have declined to follow the Restatement's limited application of the tort and, instead, broadened the tort's application.[185] Other courts rely on the state constitutional right of privacy for protection against physicians who make unauthorized disclosure of medical conditions.[186]

In addition, most states recognize a common law duty of confidentiality arising out of professional relationship[187] as applied to health care providers.[188] Thus, when a patient reasonably believes that information divulged is private, a physician may be liable for disclosure without the patient's consent or a valid justification.[189] The reasoning is that "[a] patient should be entitled to freely disclose his symptoms and condition to his doctor in order to receive proper treatment without fear that those facts may become public property. Only thus can the purpose of the relationship be fulfilled."[190] Accordingly, state courts have found a breach of confidentiality when physicians disclose information obtained from a therapeutic relationship to employers or family members.[191] For example, In *Estate of Behringer v. Medical Center at Princeton*,[192] a hospital violated its duty of confidentiality when it did not take reasonable precautions to prevent the identity of a physician who contracted HIV from becoming known to his associates and patients.[193] The court reasoned that failure to take such precautions could amount to negligence.[194] A physician may not disclose information obtained during medical visitation unless

---

184. *Id.* § 652D cmt. a.

185. *See, e.g.*, Horne v. Patton, 287 So. 2d 824, 827–30 (Ala. 1973) (holding that a physician may be liable for breach of duty of privacy when disclosing information to the patient's employer without authorization).

186. *See, e.g.*, Urbaniak v. Newton, 277 Cal. Rptr. 354 (Cal. Ct. App. 1991).

187. *See* Albert v. Devine, 479 N.E.2d 113, 120 (Mass. 1985); s*ee also* Chizmar v. Mackie, 896 P.2d 196, 207 (Alaska 1995) (discussing confidentiality as a duty of privacy arising out of a specific fiduciary relationship).

188. Gostin, *supra* note 3, at 508.

189. *Id.*

190. Hague v. Williams, 181 A.2d 345, 349 (N.J. 1962).

191. Gostin, *supra* note 3, at 509. *But see Chizmar*, 896 P.2d at 214 (holding that a physician was not liable for breach of duty of confidentiality when he reported the patient's HIV diagnosis to her husband before consulting with her because it was justified given the particular facts of the case).

192. 592 A.2d 1251 (N.J. 1991).

193. *Id.* at 1273–74.

194. *Id.* at 1272.

otherwise required by law or to protect the welfare of an individual or society.[195]

Courts also recognize a physician's contractual obligation to keep patients' information confidential.[196] Breach of contract amounts to breach of confidentiality or of privacy when the action involves disclosure of information "relating to the patient's mental or physical condition or the physician's diagnosis or treatment."[197] In *Geisberger v. Willuhn*,[198] a patient sued his physician for breach of contract when the physician's employee disclosed the patient's identity as a possible suspect of an armed robbery.[199] The court held that while a patient may sue for breach of contract, the physician did not breach his contractual duty to the patient because the disclosed information did not relate to the patient's mental or physical condition or the physician's diagnosis.[200]

Despite the tort and contract theories available to protect a patient's medical information held by physicians, "it is at best uncertain whether a duty of confidentiality extends to other health care professionals [and] researchers . . . although the risk of harm from disclosure is just as significant."[201] Apparently, the duty to protect the patient's privacy is limited to certain healthcare providers. Courts refuse to recognize a tort based on breach of confidentiality or any contract theories or duties[202] when a patient divulges personal medical information to a pharmacist.[203]

In *Evans v. Rite Aid Corp.*,[204] the plaintiff submitted a drug prescription to the defendant pharmacy and later discovered that a pharmacy employee falsely reported to others that the prescription was for medication for venereal disease.[205] The plaintiff claimed that a duty of confidence was created by statute, as well as by ethical mandate of the profession.[206] The South Carolina Supreme

---

195. *Id.* at 1268.

196. Horne v. Patton, 287 So. 2d 824, 831–32 (Ala. 1973); *see also* Albert v. Devine, 479 N.E.2d 113, 120 (Mass. 1985) (holding that a duty of confidentiality arises out of a physician-patient relationship, which creates a contractual obligation).

197. Geisberger v. Willuhn, 390 N.E.2d 945, 948 (Ill. App. Ct. 1979).

198. *Id.*

199. *Id.* at 946.

200. *Id.* at 948.

201. Gostin, *supra* note 3, at 510.

202. Suarez v. Pierard, 663 N.E.2d 1039, 1042–44 (Ill. App. Ct. 1996).

203. Evans v. Rite Aid Corp., 478 S.E.2d 846, 848 (S.C. 1996).

204. *Id.* at 846.

205. *Id.* at 847.

206. *Id.*

Court, affirming the trial court's dismissal of plaintiff's claim,[207] refused to recognize a common law duty of confidentiality between pharmacists and patients,[208] stating, "[n]o [state court] has ever recognized such a duty, nor are we aware of any other jurisdiction that has done so."[209]

In *Suarez v. Pierard*,[210] an Illinois appellate court held that a pharmacist's advice and information about the use of drugs does not establish a confidential therapeutic relationship with a patient, nor a contractual duty to protect the patient's privacy, in the absence of showing that the pharmacist was unjustly enriched.[211] In that case, the plaintiff had a prescription filled at a K-Mart pharmacy for drugs used in the treatment of mental health disorders.[212] The plaintiff disclosed confidential information to the pharmacist on duty.[213] Later, at a chance meeting with the plaintiff in a bar, the pharmacist discussed confidential information regarding her treatment in the presence of others.[214] The plaintiff, embarrassed and humiliated, sued for a breach of duty created by the state's Confidentiality Act[215] and by implied contract.[216]

The *Suarez* court first held that the Confidentiality Act does not protect a "routine transaction with a pharmacist, even where . . . the pharmacist questions plaintiff about her treatment and medical condition."[217] The pharmacist's role "is largely limited to filling the prescription as ordered by the physician . . . providing a product to a customer, not providing mental health services to a patient."[218] "Regardless of how broadly one construes the [state's] Confidentiality Act, the facts alleged here simply fail to state a cause of action [for breach of confidentiality]."[219]

The plaintiff's claim that she "entered into an implied contract whereby it was 'assumed and understood' that the

---

207. *Id.*
208. *Id.* at 848.
209. *Id.*
210. Suarez v. Pierard, 663 N.E.2d 1039 (Ill. App. Ct. 1996).
211. *Id.* at 1042–44.
212. *Id.* at 1041.
213. *Id.*
214. *Id.*
215. Mental Health and Developmental Disabilities Confidentiality Act (Confidentiality Act) 740 ILL. COMP. STAT. 110/1–17 (2000).
216. *Suarez*, 663 N.E.2d at 1041.
217. *Id.* at 1042.
218. *Id.*
219. *Id.* at 1043.

information obtained by [the pharmacist] was confidential and would not be disclosed,"[220] was summarily rejected.[221] The court refused to acknowledge that such a duty could have been implied from the facts or law.[222]

In summary, state case law protects patients' privacy against disclosure by physicians, but not by pharmacists. Such limited protection is not sufficient because pharmacists may have substantial access to patient information.

C. Congress Fails to Properly Protect Medical Privacy

Congress has failed to provide more privacy protection than do the states. In fact, although Congress self-imposed an August 21, 1999, deadline to pass new laws that set standards for protecting the confidentiality of medical records,[223] Congress failed to meet it.[224]

In 1999, Congress considered several privacy bills. On July 15, 1999, the House Committee on Government Reform Subcommittee on Government Management, Information, and Technology heard testimony[225] on the merits of House Bill H.R. 88,[226] which would have repealed the Shelby Amendment to the FOIA,[227] which limits medical privacy[228] and enhances access to federally funded research data.[229] The Shelby Amendment requires non-profit organizations conducting research to provide the government with raw data that identifies the individuals who were subject to the research, after which a government agency decides whether to allow public access to the data.[230] The data is

---

220. *Id.*
221. *Id.* at 1044.
222. *Id.*
223. Wheeler, *supra* note 40, at A21.
224. *Id.*
225. *Treasury and General Government Appropriation Act of 1999: Hearing on H.R. 88 Before the Subcomm. on Gov't Mgmt., Info. and Tech. of the House Comm. on Gov't Reform, 106th Cong.* (1999) *at* http://web.lexis-nexis.com/congcomp. [hereinafter *Hearing on H.R. 88*].
226. H.R. 88, 106th Cong. (1999).
227. Omnibus and Consolidated Emergency Supplemental Appropriations Act, Pub. L. No. 105-277, 112 Stat. 2681 (1998).
228. *See Hearing on H.R. 88*, *supra* note 225 (statement of Rep. Stephen Horn (R-Cal.), Chairman, House Subcommittee on Government Management, Information, and Technology).
229. *Id.*
230. *Id.* (statement of Bruce Alberts, M.D., President, National Academy of Sciences).

not aggregated nor edited before being sent to the agency.[231] Once the agency allows the public to access the data, it cannot place restrictions on who obtains the records or their intended use.[232] As a result, under the Shelby Amendment, violation of patient's privacy rights is permitted.[233]

While the FOIA does contain an exemption for personal medical data[234] that keeps individual names and other identifying factors confidential,[235] the FOIA is not an "appropriate mechanism" to protect patient privacy from the Shelby Amendment's required disclosure of data collected by non-private organizations[236] because the Shelby Amendment *requires* that a researcher provide the government with unedited data, at which point the agency may or may not edit the data of any personal indicators.[237] In addition, the FOIA's existing privacy mechanisms are not appropriate to protect against the Shelby Amendment because it is possible to identify the patient using non-identifying data, such as place of birth, occupation, marital status, and other general information.[238]

On July 15, 1999, the House also held a hearing on the Medical Information Protection Act of 1999.[239] The Consortium for Citizens with Disabilities (CCD), an interest group representing people with disabilities,[240] sought to have Congress require that individuals be notified in writing regarding how their medical records are used and when their individually identifiable information is disclosed to a third party.[241] The notice would have included information on the health care provider's policy for making disclosures with or without the patient's authorization, what records are being accessed, by whom, and how to refuse

---

231. *See id.*

232. *See id.* (statement of Rep. Stephen Horn (R-Cal.)).

233. *See id.* (statement of Harold Varmus, M.D., Director, National Institutes of Health, Department of Health and Human Services).

234. Freedom of Information Act, 5 U.S.C. § 552(b)(6) (1994).

235. *Hearing on H.R. 88, supra* note 225 (statement of Harold Varmus, M.D.).

236. *Id.* (statement of Bruce Alberts).

237. *Id.* (statement of Harold Varmus, M.D.).

238. *Id.*

239. *Medical Information Protection and Research Enhancement Act of 1999: Hearing on H.R. 2470 Before the Subcomm. on Health and Env't Comm. on Commerce*, 106th Cong. (1999) [hereinafter *Hearing on H.R. 2470*].

240. *Id.* at 39 (statement of Chai Feldblum, Law Professor, Director of Federal Legislation Clinic, Georgetown Law School).

241. *Id.* at 96.

authorization of disclosure, if the policy allows for patient's refusal.[242] The Act, however, would have continued to allow entities to use consumers' health information for treatment and health research without obtaining consumer authorization.[243]

Another House Bill[244] would have allowed consumers to have a reasonable opportunity to limit the use and disclosure of health information beyond the existing industry limitations on such disclosure.[245] Patients' authorization of disclosure to the third party, however, would still not be required.[246]

The CCD asked the House to require that, under the Medical Information Protection Act,[247] disclosure of *personally identifiable health information* should be allowed only "for purposes reasonably related to the purpose for which the information was collected, and for which the patient had been given notice."[248] These House Bills represent Congressional concern regarding disclosure of *identifying personal information* without the patient's consent, rather than with *anonymous information.* The CCD, hoping for more stringent limitations on health information disclosure, nevertheless indicated that the federal government should enact legislation that establishes the bare minimum required for protection of individual privacy rights,[249] leaving state legislatures the opportunity to "continue to explore ways in which to better protect the privacy of medical information in their particular states."[250]

V. AN OVERVIEW OF MEDICAL PRIVACY TRENDS

A. Medical Privacy Trends in the United Kingdom

The *Source Informatics* cases were monumental in evidencing medical privacy trends in the United Kingdom. Source Informatics argued that before the British Department of Health

242. *Id.*
243. *Id.*
244. H.R. 1941, 106th Cong. (1999).
245. *Hearing on H.R. 2470, supra* note 239, at 97.
246. *Id.*
247. H.R. 2470, 106th Cong. (1999).
248. *Hearing on H.R. 2470, supra* note 239, at 97.
249. *See id.* at 104.
250. *Id.* But as previously discussed, some states have not recognized substantial patient confidentiality rights. *See* discussion *supra* Part IV.B.

issued its policy, the publication of anonymous information to pharmaceutical countries was uncontroversial.[251] It emphasized that release of such information was not a breach of confidence.[252] Source Informatics argued that the information acquired would be not only of great commercial value to drug companies, but also would provide benefits to the medical profession by providing physicians and pharmacists useful information to monitor their prescription patterns.[253] The information would allow physicians prescribing certain medication to be informed quickly of adverse reactions, product withdrawals, or changes in prescription information.[254] In light of such benefits, the health care industry believed that providing data without identifying information did not create legal liability.[255]

Contrary to Source Informatics' assertion, however, a controversy over this exact issue did exist within the medical community even before the British Department of Health issued its policy statement.[256] Although data collection companies did not need the consent of patients to access their prescription information, they did require the consent of both the physicians and pharmacists who maintained the data.[257] In practice, however, some companies may have acquired the information without the consent of the physicians or pharmacists.[258] Additionally, even when proper consent was obtained, pharmacists and physicians were not able to review the information they were submitting to data collection companies, potentially giving the companies greater access to information than intended.[259] Accordingly,

---

251. R. v. Dep't of Health *ex parte* Source Informatics Ltd., 4 All E.R. 185, 189 (Q.B. 1999), *rev'd*, 1 All E.R. 786 (C.A. 2000).

252. 4 All E.R. at 188.

253. *Prescription Information Remains Confidential, supra* note 48, at 45.

254. John Aston, *Database Company Seeks Right to Sell Prescription Details*, PRESS ASS'N NEWSFILE, May 18, 1999.

255. *See Pharmacy World, supra* note 46, at 3.

256. *See generally* Norton, *supra* note 11, at 10 (finding troubling confidentiality problems with Source Informatics' data collection procedures).

257. *Prescription Information Remains Confidential, supra* note 48, at 45.

258. Norton, *supra* note 11, at 10. The newspaper acquired a copy of information provided to data companies, which identified names of several physicians who prescribed medications. *Id.* Of the two physicians in the list that were contacted by the newspaper, neither consented to the sale of information. *Id.* Nonetheless, a Source Informatics' spokesperson stated that the information it obtained was acquired according to proper procedure. *Id.*

259. *Id.*

concerns regarding the information obtained by data collection companies already existed before the British Department of Health issued its statement.

In a 1996 newspaper article adopted from a speech, Sir Thomas Bingham, Lord Chief Justice, stated that in the United Kingdom there was "no recognition of a general right to privacy."[260] He noted, however, that the courts recently "have extended the remedy for breach of confidence to afford a measure of protection for rights of personal privacy."[261] Yet, despite the existing Common Law and recent statutory privacy provisions, "there are other [situations] in which privacy is infringed and to which [existing laws] do not apply, leaving the victim without a remedy."[262] Chief Justice Bingham recommended that Parliament enact a law that would protect the rights of personal privacy to a greater extent than the current laws.[263] Specifically, the law should affect significant privacy infringements such as those that "would cause substantial distress to an ordinary phlegmatic person."[264] If the legislature failed to pass such general privacy legislation, he predicted that the courts would protect additional privacy rights in future cases.[265]

The *Source I* court gave effect to the Chief Justice's prediction when it decided that Source Informatics was infringing upon patients' rights to privacy by collecting and releasing anonymous medical data.[266] The court noted that while it is common knowledge that data taken from patients' records is routinely used for medical research and literature as well as for obtaining statistics,[267] such practices violate privacy rights.[268] For public policy reasons, the court deemed the release of such information a breach of confidence.[269]

This decision had several immediate consequences. The Royal Pharmaceutical Society of Great Britain followed the

---

260. Bingham, *supra* note 45, at T16.
261. *Id.*
262. *Id.*
263. *See id.*
264. *Id.*
265. *Id.*
266. *See* Norton, *supra* note 11, at 10.
267. R. v. Dep't of Health *ex parte* Source Informatics Ltd., 4 All E.R. 185, 189 (Q.B. 1999), *rev'd*, 1 All E.R. 786 (C.A. 2000).
268. 4 All E.R. at 197.
269. *Id.* at 196–98.

British Health Department's policy and advised pharmacists not to provide data to collection companies.[270] In addition, the British General Medical Council (GMC), intending to issue policy guidance for physicians that allowed them to obtain *implied consent* from patients to disclose records for medical research simply by posting waiting room posters and practice leaflets,[271] postponed the publication of the guidelines to await the results of Source Informatics' appeal.[272]

After the trial court issued its ruling, GMC believed that the decision only applied to patient data provided to commercial companies and not to the record sharing within the National Health Service for research and audit.[273] For instance, it was asserted that a physician may be able to disclose anonymous information to report adverse drug reactions and not come under this ruling because the information was disclosed for public interest, rather than for commercial purposes.[274] The ruling, therefore, created uncertainty regarding whether all use of anonymous data was prohibited or only use of the data for pecuniary purposes.[275]

On appeal, the *Source II* court took a different position when it reversed the trial court's decision[276] and refused to recognize the patient's right to privacy in anonymous medical data.[277] Interestingly, the court acknowledged that, in the United Kingdom, a pharmacist owes a duty of confidentiality to a patient.[278] As discussed below, the duty owed by a pharmacist to a patient receives little attention in the United States.[279]

---

270. *Pharmacy World*, *supra* note 43, at 3.

271. Thomlinson & Thakor, *supra* note 21, at 1.

272. Lisa Tomlinson, *Law Enforcer Doubts GMC Disclosure Rules*, PULSE, Aug. 21, 1999, at 3.

273. Thomlinson & Thakor, *supra* note 21, at 1.

274. *Make Sure of Security Needs*, *supra* note 52, at 21.

275. *See id.*

276. *See* R. v. Dep't of Health *ex parte* Source Informatics Ltd., 1 All E.R. 786, 797 (C.A. 2000), *rev'g* 4 All E.R. 185 (Q.B. 1999).

277. 1 All E.R. at 797. "[C]ourts . . . should not be too ready to import an equitable obligation of confidence in a marginal case." *Id.* at 794 (citing Smith Kline & French Labs. (Austl.) Ltd. v. Sec'y to the Dep't of Cmty. Servs. and Health, 99 A.L.R. 679, 691–92 (1991)).

278. 1 All E.R. at 796 (noting that a pharmacist is a "confidant [who] is placed under a duty of good faith to the confider").

279. *See* discussion *supra* Part IV.B.2.

B. Medical Privacy Trends in the United States

1. Rights Sought in the United Kingdom Remain Unchallenged in the United States

Although U.S. law protects some personal data from unwarranted invasion, the law does not recognize individual personal data as an interest that needs substantial protection.[280]

The general public, on the other hand, far from being passive about protections afforded to anonymous medical data gathered for marketing and other research, is concerned about medical privacy and protecting the confidentiality of patient records.[281] According to the 2000 Gallup Poll conducted on behalf of the Institute for Health Freedom, the vast majority of U.S. residents oppose allowing third parties access to medical data without patient permission.[282] Many individuals oppose access by any group[283] and sixty-seven percent of adults polled indicated that they would oppose access to medical researchers.[284]

While medical privacy does receive some protection in the United States,[285] these protections are superficial.[286] Moreover, not only do U.S. laws fail to protect non-identifiable information, privacy bills considered by Congress in 1999 explicitly permit release of such information.[287] Consequently, unlike the United

---

280. *See* Roch, *supra* note 33, at 93. Federal laws are subject to numerous exceptions and apply to limited types of data. *See id.* at 88–93.

281. Gostin, *supra* note 3, at 453–54.

282. *See* THE GALLOP ORGANIZATION, *supra* note 116.

283. *Id.*

284. *Id.*

285. *See* discussion *supra* Part IV.

286. *See* Rackett, *supra* note 166, at 178–83. In addition, few states have enacted comprehensive medical confidentiality laws and those in effect are subject to disclosure exceptions. *Id.* at 181–83. *See also* Helena Gail Rubinstein, *If I Am Only for Myself, What Am I?: A Communitarian Look at the Privacy Stalemate*, 25 AM. J.L. & MED. 203, 203 (1999) ("U.S. Senator Edward M. Kennedy asserts, '[t]oday, video rental records have greater protection than sensitive medical information.'") (alteration in original).

287. *See* Rubinstein, *supra* note 286, at 220. Several recent federal medical privacy bills required only that identifiable information be protected. The Medical Privacy and Security Act, S. 573, 106th Cong., 1st Sess. (1999), sponsored by Senator Patrick Leahy (D-Vt.), required that all personal identifiers be removed before disclosure is permitted. Rubinstein, *supra* note 286, at 219. The Health Care Personal Information Non-Disclosure Act, S. 578. 106th Cong. 1st Sess. (1999), sponsored by Senator James Jeffords (D-Vt.) and Senator Chris Dodd (D-Conn.), permits the disclosure of information but requires that the data does not reveal the identity of the patient. Rubinstein, *supra* note

Kingdom, the lack of privacy protection in non-identifying data has not been challenged in the United States.[288]

2. New Database Creates Risks That Medical Information Is Being Misused

In the United States, patient records are increasingly maintained and transmitted electronically, allowing insurance companies, hospitals, physicians, and pharmacists to exchange information about patients.[289] Health database organizations, with their chief goal of publicly releasing and analyzing information, have accelerated the collection, storage, and use of electronic data.[290] The information obtained includes patient-identifiable data, as well as aggregate, non-identifiable data.[291] These organizations can legally use and sell the data for numerous purposes that a patient would not anticipate when the data is collected.[292] The list of groups using patient computerized records is exhaustive.[293] Accordingly, the issue is to what extent should a third party be allowed to access a patient's medical records?[294]

According to a Congressional Research Service study, at least 400 people legally have access to a patient's records during an average hospital stay.[295] The current availability of medical information raises the possibility that the data may fall into the hands of groups who might use it for inappropriate purposes.[296] Hence, some scholars wonder whether too little has been made of

---

286, at 219. The Medical Information Protection Act of 1999, S. 881, 106th Cong., 1st Sess. (1999), introduced by Senator Robert Bennett (R-Utah), explicitly permits disclosure of data from which direct identifiers have been removed. Rubinstein, *supra* note 286, at 219.

288. Exhaustive research for this Note revealed that the use of anonymous data has remained unchallenged in U.S. federal, state, and case law. Indeed, the trial court in *Source I* indicated that this was a novel legal issue. R. v. Dep't of Health *ex parte* Source Informatics Ltd., 4 All E.R. 185, 189 (Q.B. 1999), *rev'd*, 1 All E.R. 786 (C.A. 2000).

289. Wheeler, *supra* note 40, at A21.

290. Gostin, *supra* note 3, at 463.

291. *Id.* at 464.

292. *Id.* at 488.

293. *Id.* at 485–86.

294. Kasper Zeuthen, *Health Information Moves Too Freely in United States*, THE DAILY YOMIURI, Sept. 7, 1999, at 7.

295. *Id. Cf.* Rackett, *supra* note 166, at 173 (estimating at least eighty people).

296. *See* Chadwick, *supra* note 109, at 443. For example, in 1996, thirty-five percent of the Fortune 500 companies acknowledged that they used personal health information in making employment decisions. Zeuthen, *supra* note 294, at 7. In 1992, U.S. Representative Nydia Velazquez's hospital records were anonymously released to the press in attempt to sabotage her bid for a Congressional seat. *Id.*

the threat to individual privacy posed by medical information systems.[297]

New medical records databases are continually established for greater convenience of medical service providers and patients.[298] On August 23, 1999, WellMed, Inc., a privately held company in Portland, announced that corporations as well as health plans and care service providers would begin utilizing its online personal health database,[299] the Personal Health Manager, which allows consumers to store and retrieve information that is customized to their own health interests or medical conditions.[300] The database allows individuals to store and monitor health information online, as well as maintain children's immunization records and elderly patients' prescriptions, which can easily be accessed and provided to schools, new doctors, and others.[301] The program allows for storage of information online with "complete security, confidentiality[,] and privacy."[302] In case of emergency, however, a company operator can access the information and fax the customer's Emergency Information to the "appropriate contact at the hospital."[303] One must question how *private* the data is when it is exposed to so many people, especially considering that the data being processed can be directly linked to an identifiable person.

In addition, virtual drugstores, selling prescription and non-prescription drugs, are a new trend on the Internet.[304] Most major websites promise that they "'will not sell, rent[,] or loan any *recognizable personal information* to a third-party, unless legally required to do so.'"[305] Thus, when a customer or patient provides medical information to healthcare Web sites, anonymous information might still be given to a third party.

---

297. *See* Lombardo, *supra* note 118, at 589.

298. *See WellMed Introduces Industry's First Comprehensive Personal Health Management System Including Online Health Record*, PR NEWSWIRE, Aug. 23, 1999, *available at* LEXIS, News Library, Allnws File [hereinafter *WellMed*].

299. *Id.*

300. *Id.*

301. *Id.*

302. *Id.*

303. *Id.*

304. Stephanie Harvin, *http://www.drugs.com*, THE POST AND COURIER, Aug. 2, 1999, at 8-B.

305. *Id.* (emphasis added).

VI. UNLIKE THE UNITED KINGDOM, THE UNITED STATES SHOULD AFFORD PROTECTION FOR PRIVACY IN ANONYMOUS DATA

The outcome of the *Source II* decision is not surprising because there are public health benefits in providing access to patients' records to certain third parties.[306] Personal medical records available on Web sites, such as the one offered by WellMed,[307] allow patients to access diagnoses from home.[308] Doctors dealing with patients' ailments could obtain prescription records, the nature of the complaint, and the history of the treatment online, then diagnose potential reasons for the complaint.[309] General medical records databases give physicians insight to develop new disease prevention strategies, treatments, and cures.[310] These databases can also help scientists study the evolution of hereditary diseases.[311] Furthermore, researchers improve the quality of health care by analyzing personal identifiable prescription information, identifying patients who might be eligible for a change in their prescription, and contacting the physicians treating these patients.[312]

Nevertheless, the British appellate court took a step backward for the protection of privacy rights by adopting the "reasonable pharmacist" standard, which permits a pharmacist to disclose anonymous data to an unauthorized third party so long as it would not be unconscionable to a reasonable pharmacist.[313] The court should have (1) recognized a privacy right in anonymous data, (2) considered whether a reasonable person would oppose use of the data, and (3) determined whether there are public policy reasons to outweigh the individual privacy rights. The appellate

---

306. *See* Wheeler, *supra* note 40, at A21 (noting that some researchers claim to need access to medical records to properly conduct research).

307. *WellMed*, *supra* note 298.

308. Pam Abramowitz, *Computerized Patient Records: Health Care Finally Moves to Place the Consumer at the Center of its IT Revolution*, THE BOND BUYER (Health Care Finance Supp.), Sept. 1999, at 12a.

309. *Id.*

310. Lawrence O'Rourke, *Are Your Private Records Private?*, TOPEKA CAP. J., June 15, 1999, *available at* LEXIS, News Library, Allnws File.

311. *Id.*

312. *Medical Records Confidentiality in the Modern Delivery of Health Care: Hearing Before the Subcomm. on Health and Env't of the House on Commerce*, 106th Cong. 69 (1999) (prepared statement of Terry S. Latanich, Senior Vice-President of Mercko-Medco Managed Care) (providing an example of how patient-identifiable information is used).

313. R. v. Dep't of Health *ex parte* Source Informatics Ltd., 1 All E.R. 786, 797 (C.A. 2000), *rev'g* 4 All E.R. 185 (Q.B. 1999).

court's analysis, however, rejected these important principles used by U.S. courts, which were argued by the British Department of Health in the *Source Informatics* cases.

First, the *Source II* court reasoned that when a patient can be assured that identifying information will be protected, that patient has no interest in how anonymous data is used.[314] The appellate court's definition of privacy conforms with the limited definition used by some scholars who propose that privacy is invaded only when identity is revealed.[315] Other scholars, such as Charles Fried, however, argue that privacy is a fundamental notion that must not be easily disturbed.[316] A primary justification for respecting the privacy of an individual is the principle of respect for the individual's autonomy.[317] An individual should have the autonomy to decide who gets to use personal data.[318] For Fried, therefore, privacy is lost immediately when a person loses the ability to grant or deny access to information, whereas other scholars allow third parties to access information without authorization as long as the patient is not identified.

Both the *Source I* and *Source II* courts acted under the presumption that anonymity can be guaranteed.[319] In reality, however, "complete anonymity is extraordinarily difficult, if not impossible, to attain[,]"[320] because even in the absence of identifying information, it is possible to aggregate data to determine the person's identity.[321] Assuming, however, that anonymity can be guaranteed, the exposure of the patient's identity is not the only possible circumstance that can raise a cause of action for invasion of privacy.[322] Courts have recognized that

---

314. 1 All E.R. at 797.

315. Gostin et al., *supra* note 38, at 18–19 (noting that some scholars define privacy as the condition of limited accessibility to the person such that it does not encroach on the person's solitude, secrecy, and anonymity, suggesting that privacy is not invaded if the person's anonymity is guaranteed).

316. *See* Fried, *supra* note 1, at 477–78.

317. Gostin et al., *supra* note 38, at 21.

318. *Id.* at 19 (noting that a lack of control over who may use a person's information, such as when a person is subjected to an involuntary blood test, results in the loss of "decisional privacy").

319. R. v. Dep't of Health *ex parte* Source Informatics Ltd., 1 All E.R. 786, 789 (C.A. 2000), *rev'g* 4 All E.R. 185 (Q.B. 1999).

320. Wheeler, *supra* note 40, at A24.

321. *Id.*

322. *See, e.g.*, Roe v. Wade, 410 U.S. 113, 153 (1973) (noting that the right to privacy encompasses "a woman's *decision* whether or not to terminate her pregnancy") (emphasis

an invasion of privacy does not necessarily involve identity, but rather occurs when a person is deprived of the autonomy to make decisions.[323] Therefore, even if the anonymity is guaranteed, invasion of privacy occurs when the patient is deprived of the autonomy to determine how the information is used.[324]

Second, once the law recognizes that a person has an interest in protecting access to information, whether anonymous or identifiable, not every use of that information violates the right to privacy.[325] Only unauthorized access to the information that would offend a reasonable person's expectations for the use of the information would violate that right.[326] This indicates that invasion of privacy exists when a reasonable person would object to the use. The problem that the appellate court's ruling raises is determining whether to use a reasonable patient standard or that of a reasonable pharmacist.[327]

In both invasion of privacy and breach of confidentiality cases, it makes more sense to use a reasonable patient standard. Although it is common in tort law, such as in malpractice claims, to apply the "reasonable professional" standard,[328] the right of privacy is an individual right that should be defined from the viewpoint of the victim of the breach, not its perpetrator.[329] Arguably any use of data that is unauthorized or even unknown to the patient could be objectionable to a reasonable patient. This view would be in conformity with the Restatement (Second) of Torts, which defines invasion of privacy as publication of information that is "highly offensive to a reasonable person[,]"[330] namely the patient. This is not the view adopted by the appellate

---

added).

323. *See id.*

324. *See* Fried, *supra* note 1, at 482.

325. *See* R. v. Dep't of Health *ex parte* Source Informatics Ltd., 1 All E.R. 786, 796 (C.A. 2000), *rev'g* 4 All E.R. 185 (Q.B. 1999).

326. RESTATEMENT (SECOND) OF TORTS § 652D(a) (1977). *But see Source Informatics Ltd.*, 1 All E.R. at 796 (holding that a reasonable pharmacist standard should be applied).

327. *See, e.g.*, Urbaniak v. Newton, 277 Cal. Rptr. 354, 361 (Cal. Ct. App. 1991) (noting that the patient's "reasonable expectations of privacy" would determine whether the privacy interest deserves protection against abusive disclosure of data).

328. *See, e.g.*, Osborn v. Irwin Memorial Blood Bank, 7 Cal. Rptr. 2d 101, 127–28 (applying a standard of reasonable degree of care exercised by other blood banks in a malpractice case).

329. *See, e.g.*, *Urbaniak*, 277 Cal. Rptr. at 361 (using a reasonable patient standard).

330. RESTATEMENT (SECOND) OF TORTS § 652D(a) (1977).

court in *Source II*.[331] The court, instead, took the view that a pharmacist improperly discloses the information only when a reasonable *pharmacist* would find the disclosure to an unauthorized party unconscionable.[332]

Third, once the patient's interest in the data is recognized, it may be proper to invade privacy rights when public interest outweighs the personal right.[333] The *Source II* court, instead of recognizing privacy rights in anonymous data and weighing them against the public interest in the data, denied the existence of the patient's privacy interests and allowed the publication of the data regardless of the weight of public interest.[334]

Contrary to the *Source II* decision in the United Kingdom, the law in the United States weighs public policy considerations against the individual right to privacy.[335] In the United States, once the duty of confidentiality arises, the existence of that duty does not preclude publicizing confidential information when the public interest in the data outweighs the patient's right to privacy.[336] There may be a significant public policy reasons to allow a pharmacist to sell anonymous data for use by third parties.[337] For instance, modern medicine might not exist without the wide distribution of medical data between different segments of the medical community.[338]

The *Source Informatics* cases, however, involved data distribution for purely pecuniary purposes, rather than for research.[339] While a U.S. court might decide that pecuniary need for the data does not outweigh patients' privacy rights,[340] the

---

331. *See Source Informatics Ltd.*, 1 All E.R. at 797.

332. *Id.*

333. *See, e.g.*, Urbaniak, 277 Cal. Rptr. at 360–61 (holding that the public's interest in the disclosure of a patient's HIV-positive status for the purpose of alerting a healthcare worker of the need for safety precautions outweighs the patient's privacy rights).

334. *See Source Informatics Ltd.*, 1 All E.R. at 796–97.

335. *See, e.g.*, United States v. Westinghouse Elec. Corp., 638 F.2d 570, 578 (3d Cir. 1980); *see also Urbaniak*, 277 Cal. Rptr. at 361.

336. *Westinghouse*, 638 F.2d at 578.

337. *See* Rubinstein, *supra* note 286, at 224–31, for a discussion on communitarian policy reasons to allow use of medical data without the patient's consent.

338. *See* Gostin, *supra* note 3, at 451–52.

339. *See Source Informatics Ltd.*, 1 All E.R. at 788 (noting that Source Informatics buys the data and resells it to pharmaceuticals so that they can better market their products).

340. *See, e.g.*, Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 657 (Cal. 1994) (requiring sufficient countervailing interests to outweigh the right to privacy under the California state constitution); Stenger v. Lehigh Valley Hosp. Ctr., 530 Pa. 426, 437 (1992)

British appellate court was not concerned with the weight of public policy considerations.[341] Instead, the British court held that patients have no property interests in anonymous data.[342] Thus, in the United Kingdom, a patient cannot object when the data is used for unauthorized purposes by third parties.[343]

Courts should recognize that use of anonymous information violates patients' privacy. In suggesting comprehensive U.S. federal legislation to protect medical privacy, scholars have advanced several principles for fair information practices.[344] Included are the principles that information should be collected only for the purpose for which it was intended and should not be used for other purposes without the patient's consent.[345] These principles should be used equally for identifiable as well as non-identifiable data because the patient did not consent to the use of the data by third parties.

Furthermore, privacy should be defined as the right to control access to information[346] because this definition provides greater protection against unauthorized use. Additionally, to ensure that doctors, pharmacists, and interested third parties respect patient privacy, patients should be able to state a claim against anyone who accesses private information. In the United Kingdom, medical personnel other than physicians, such as pharmacists, can be liable for breach of confidentiality for making identifiable information public,[347] but in the United States, the pharmacist cannot be held liable.[348] This prevents a U.S. patient from

---

(requiring compelling state interests to outweigh a person's privacy rights under the Pennsylvania state constitution).

341. *Source Informatics Ltd.*, 1 All E.R. at 790.

342. *Id.* at 797. Generally, U.S. laws state that medical records are the sole property of the health care provider. Rubenstein, *supra* note 286, at 207. This view mirrors the British appellate court's holding that the patient has no property rights in anonymous data. *Source Informatics Ltd.*, 1 All E.R. at 797. Most states, however, require health care professionals to ensure the patient's confidentiality and therefore do not give these professionals an absolute right to use the information. Rubenstein, *supra* note 286, at 207–08. It is unknown whether a U.S. court would require the same duty of confidentiality for anonymous data.

343. *Source Informatics Ltd.*, 1 All E.R. at 796–97.

344. Rackett, *supra* note 166, at 188.

345. *Id.*

346. Fried, *supra* note 1, at 483.

347. *Source Informatics Ltd.*, 1 All E.R. at 796.

348. *See* discussion *supra* Part IV.B.

controlling access to information, thus any data held by a non-physician can potentially become public.[349]

Courts should recognize that *all* unauthorized use of that data is, by definition, an invasion of privacy. The patient is deprived of the right to control access to the information, which is detrimental to the patient's rights.[350] Although courts should be able to allow disclosure if the public interest in the information is strong, the public interest must involve a social necessity that outweighs the basic individual right of privacy.[351] The interest of a company in the data to better market its products, for example, should not be compelling enough to overcome the fundamental right of privacy.

Finally, in deciding whether privacy rights are violated when a pharmacist divulges anonymous data to a third party without the patient's consent, courts should use a *reasonable patient* standard, not a *reasonable pharmacist* standard.[352] The question is not whether the pharmacist violated a professional duty to a client, but rather, whether the pharmacist violated a patient's fundamental right to control access to personal information.[353] Although the *Source I* court did limit the ability of a pharmacist and physician to use the data, it did so nominally. The reasonable pharmacist standard does not permit the pharmacist to use data in a way that a reasonable pharmacist would find unconscionable,[354] but what amounts to unconscionable is restricted only by the subjective need of the medical community that uses the data in an unauthorized manner. A claim for invasion of privacy should not be defined from the viewpoint of the invader; rather it should be based on the viewpoint of the victim. By definition, invasion of privacy involves the victim's sense of violation, not the professional's sense of unconscionability.[355]

---

349. *See, e.g.*, Evans v. Rite Aid Corp., 478 S.E.2d 846 (S.C. 1996).

350. Fried, *supra* note 1, at 485 ("To be deprived of this control not only over what we do but over who we are is the ultimate assault on liberty, personality, and self-respect.").

351. R. v. Dep't of Health *ex parte* Source Informatics Ltd., 4 All E.R. 185, 196 (Q.B. 1999), *rev'd*, 1 All E.R. 786 (C.A. 2000) (suggesting that if public policy could outweigh privacy interests, the sale of patient prescription data would be allowed).

352. *Compare Source Informatics Ltd.*, 1 All E.R. at 796 (using a reasonable pharmacist standard) *with* Urbaniak v. Newton, 277 Cal. Rptr. 354, 361 (Cal. Ct. App. 1991) (using a reasonable patient standard).

353. *See* Fried, *supra* note 1, at 483.

354. *Source Informatics Ltd.*, 1 All E.R. at 796.

355. *See id.*

VII. CONCLUSION

Medical data that is obtained by physicians and pharmacists specifically to provide care to the patient must not be given to unauthorized third parties unless the public needs outweigh the patient's privacy rights. The patient parted with the data for that specific purpose and must be able to retain the ability to control who accesses it. Loss of that control amounts to loss of privacy rights. Therefore, the lower court reached the proper decision in *Source I* when it held that unauthorized use of anonymous data, in the absence of a showing of a strong public interest, violates patients' right to privacy.[356] In reversing the trial court, the appellate court not only limited patients' rights, it created a precedent where the role of public policy is ignored and patients' interests are subjugated in favor of the medical community's commercial interests.

Yaron F. Dunkel *

356. R. v. Dep't of Health *ex parte* Source Informatics Ltd., 4 All E.R. 185, 196–97 (Q.B. 1999), *rev'd*, 1 All E.R. 786 (C.A. 2000).

* J.D. candidate, Loyola Law School, Los Angeles, 2001; B.A., University of California, Los Angeles, 1997. I dedicate this Note to my parents, Jacob and Martine, whose love, devotion, support, and encouragement cannot be surpassed. I am also thankful to the editors and staff of the *Loyola of Los Angeles International and Comparative Law Review* for their hard work and helpful suggestions. I am especially grateful to Ronda McKaig, Emery Shiau, Dan Loritz, and Jean Yasuhara Law for the tireless efforts they invested in this Note.